Ministerul Public – Parchetul de pe lângă Înalta Curte de Casație și Justiție

Parchetul General Bulgaria

Parchetul General Ungaria

HOME/2010/ISEC/AG/INT – 006
„Consolidarea cooperării dintre organele de aplicare a legii şi sectorul privat în scopul combaterii fraudei şi a comerţului ilegal de pe internet”

Linii directoare privind cele mai bune practici
Cooperarea dintre Organele de Aplicare a Legii şi Furnizorii de Servicii de Internet

Manual pentru punerea în practică în România, Bulgaria și Ungaria

Cu sprijinul financiar al Programului Prevenirea şi Combaterea Criminalităţii al Uniunii Europene, Comisia Europeană - Directoratul General Afaceri Interne

HOME/2010/ISEC/AG/INT – 006
„Consolidarea cooperării dintre organele de aplicare a legii şi sectorul privat în scopul combaterii fraudei şi a comerţului ilegal de pe internet”

Redactat de:

Cormac Callanan (Irlanda) E-mail: cormac.callanan@aconite.com
Peter Robbins OBE, QPM (Marea Britanie)
E-mail: peter.robbins@btinternet.com

Prezentul raport a fost redactat cu finanţarea ISEC a Directoratului General Afaceri Interne.

Această publicație reflectă părerile autorilor, iar Comisia Europeană nu poate fi trasă la răspundere pentru conținutul acestui manual și pentru părerile exprimate în cadrul acestui document.

Cu sprijinul financiar al Programului Prevenirea şi Combaterea Criminalităţii al Uniunii Europene, Comisia Europeană Directoratul General Afaceri Interne

Autorii

CORMAC CALLANAN – IRLANDA

Cormac Callanan este directorul Aconite Internet Solutions (www.aconite.com), furnizor de expertiză în ceea ce priveşte elaborarea de politici în domeniul criminalităţii informatice şi al securităţii şi siguranţei pe internet.
Licenţiat în informatică, are peste 25 de ani de experienţă profesională în domeniul reţelelor internaţionale de calculatoare şi 10 ani de experienţă în domeniul criminalităţii informatice. A furnizat pregătire pentru Interpol şi Europol şi pentru agenţiile de aplicare a legii de peste tot din lume. În prezent furnizează servicii de consultanţă la nivel mondial şi a lucrat pe elaborarea de politici în cadrul Consiliului Europei şi al Oficiului Națiunilor Unite pentru Droguri și Crimă.
În 2008 a finalizat un studiu de linii directoare privind cele mai bune practici, aplicabile cooperării dintre furnizorii de servicii şi organele de aplicare a legii, în scopul combaterii criminalităţii informatice (www.coe.int/cybercrime).
În 2009 a produs cele mai bune practici internaţionale pentru elaborarea de profiluri de studiu 2Centre (Centre de excelenţă de cercetare, pregătire şi educare în domeniul criminalităţii informatice) pentru pregătirea experţilor criminalişti din cadrul Organelor de Aplicare a Legii pe IT (www.2centre.eu).
În 2009 a fost co-autorul unui raport intitulat Blocarea Internetului – echilibrarea reacţiilor la adresa criminalităţii informatice din societăţile democratice, care explică ce reprezintă blocarea internetului, care sunt motivaţiile care stau la baza blocării internetului în societate şi care sunt aspectele de natură juridică ce au impact asupra strategiilor de blocare a internetului.
În 2010 a fost co-autorul unui raport intitulat Să Sari Peste Zidul de Protecţie – trecerea în revistă a instrumentelor de evitare a cenzurii (Leaping over the Firewall: A Review of Censorship Circumvention Tools), care oferă o comparaţie a diferitelor instrumente de evitare, după meritele tehnice, dar şi după experienţa pe care o au utilizatorii cu aceste instrumente.
De 8 ani, Cormac este preşedintele şi directorul executiv al INHOPE – Asociaţia Internaţională a Liniilor Verzi de pe Internet (www.inhope.org), coordonând activitatea liniilor verzi de pe internet care reacţionează la utilizarea/ conţinutul ilegal de pe internet. A fost co-autorul primului Raport al INHOPE privind tendinţele globale de pe internet din 2007, publicaţie de referinţă în domeniul pornografiei infantile de pe internet. A fost preşedintele Consiliului de Administraţie al Asociaţiei Europene a Furnizorilor de Servicii de Internet (EuroISPA).

Peter Robbins OBE, QPM - Marea Britanie

Peter Robbins este expert independent neafiliat, consilier, evaluator şi consultant specializat în materia conţinutului cu caracter penal şi inadecvat pe internet, care militează pentru promovarea de parteneriate publice private pentru combaterea criminalităţii online.

Timp de 30 de ani a lucrat pentru Serviciul de Poliţie Metropolitană şi şi-a încheiat cariera cu gradul cel mai înalt din poliţie, răspunzând de unul dintre cartierele londoneze. Când a lucrat în poliţie, a fost promovat pe diferite funcţii, dobândind experienţă operativă, de anchetă şi strategică.

A fost numit Directorul Executiv al Fundaţiei Internet Watch în 2002.

A condus respectiva organizaţie de auto-reglementare din sectorul privat, care a adoptat o perspectivă de parteneriat cu Guvernul Britanic, Organele de Aplicare a Legii şi o multitudine de Furnizori de Servicii de Internet, operatori de reţele mobile, furnizori de căutări şi sectorul financiar care combat la nivel global conţinutul cu caracter penal, în special abuzul sexual al copiilor (pornografie infantilă) de pe internet. Peter a controlat creşterea numărului de membri de la doar 15 societăţi comerciale la aproape 200, majoritatea acestora fiind firme bine cunoscute în toată lumea şi la nivel european.

A fost membru în Forumul Marii Britanii pentru Criminalitatea de pe Internet, un forum inter-instituţional (cu factori implicaţi din domeniul public şi de stat) cu scopul de a re-examina şi comenta pe marginea politicii de combatere a criminalităţii online aplicate la nivel naţional. A fost, de asemenea, membru al Consiliului de Administraţie al Consiliului Marii Britanii pentru Siguranţa Online a Copiilor şi a fost, de asemenea, membru al Grupului Multidisciplinar de Acţiune al Ministrului de Interne pentru Protecţia Copiilor pe Internet. A prezidat un grup naţional de furnizori de metode de căutare, în numele guvernului, care a publicat un ghid de bune practici pentru furnizorii de metode de căutare pe internet şi pentru utilizatorii internetului.

I-a fost acordată Medalia Reginei pentru activitatea din poliţie (QPM) în 2001 pentru merite deosebite în activitatea de poliţie şi a mai primit, de asemenea, şi onoarea din partea Reginei, de a-i fi fost acordat în 2008 Ordinul Imperiului Britanic pentru serviciile aduse copiilor şi familiilor acestora.

TABLĂ DE MATERII

Rezumat general

Prezentul manual include paşii detaliaţi pentru a fi de ajutor la crearea dialogului dintre sectoarele public şi privat în scopul dezvoltării unei culturi a cooperării şi la redactarea de formulare de solicitare de date standard pentru a obţine informaţiile deţinute de firmele private în scopul de a le prelucra în vederea desfăşurării urmăririi penale. Se adresează procurorilor, personalului organelor de aplicare a legii şi reprezentanţilor furnizorilor de servicii de internet, instituţiilor financiare şi furnizorilor de servicii din societatea informaţională, inclusiv furnizorilor de comerţ electronic.

În cursul elaborării prezentului manual au fost organizate două ateliere la care au participat cel puţin şaisprezece procurori şi ofiţeri de poliţie specializaţi pe combaterea criminalităţii online din România, Bulgaria şi Ungaria, trei membri ai asociaţiilor de furnizori de servicii de internet şi mai mulţi furnizori de servicii de internet care, împreună, pun la dispoziţie un set de diferite servicii online. Ulterior a fost organizată o masă rotundă pentru validarea şi diseminarea rezultatelor proiectului, care a inclus pe mulţi dintre participanţii la activităţile anterioare şi reprezentanţi ai personalului organelor de aplicare a legii/ furnizori de servicii de internet din cel puţin alte cinci State Membre UE din Europa Centrală şi de Est.

Înşelăciunile şi comerţul ilegal de pe internet sunt fapte penale din ce în ce mai răspândite. Deoarece criminalitatea online nu cunoaşte graniţe, urmărirea penală cu succes a acestor fapte necesită contribuţia suplimentară a furnizorilor de servicii de internet şi a altor actori din sectorul privat.

În prezent, nivelul şi eficacitatea cooperării dintre organele de

aplicare a legii şi sectorul privat ar putea fi descrise cel mai bine ca variind. Uneori, datele furnizate legal anchetatorilor din organele de aplicare a legii, procurorilor publici, de către deţinătorii datelor din sectorul privat, nu pot fi folosite ca probatoriu, deoarece sunt fie incomplete, fie prezentate într-un format necorespunzător pentru multitudinea de instanţe diferite de la nivelul mondial. Această situaţie poate conduce la întârzieri substanţiale cu ancheta şi urmărirea penală pentru infracţiuni cuprinse în sfera infracţională online, precum şi la irosirea resurselor valoroase ale actorilor din sectoarele public şi privat.

Cultura cooperării

Consiliul Europei a publicat în 2008 linii directoare cuprinzătoare (Anexa I – Linii directoare) încurajându-i pe furnizorii de servicii de internet şi pe organele de aplicare a legii să coopereze mai îndeaproape. Există probe clare că documentul cuprinzând liniile directoare a fost tradus în multe limbi şi a circulat la scală largă, însă tot au mai rămas anumite aspecte care trebuie să fie convertite în contextul naţional pentru a avea avantaje în practică. Sperăm ca următorii paşi să poată fi de ajutor pentru acest proces, şi anume, de a pune în practică liniile directoare.

Ar fi de dorit ca România, Bulgaria şi Ungaria să acorde atenţie:

- organizării diseminării liniilor directoare ale Consiliului Europei la nivelul autorităţilor publice (poliţie, parchete) şi să se asigure că toţi membrii personalului sunt la curent cu acestea
- verificării stadiului de cooperare dintre autorităţi şi sectorul privat, după care să îmbunătăţească această cooperare cu ajutorul instituirii de metode controlate, clare, de cooperare la nivel naţional

- strângerii la un loc a tuturor învăţămintelor trase pentru a îmbunătăţi cooperarea internaţională (după ce nivelul naţional de cooperare va fi suficient de organizat).

Controalele de calitate, prioritizarea şi proporţionalitatea în legătură cu solicitările de date reprezintă aspecte cheie dacă pe viitor trebuie gestionate într-un mod eficient şi eficace solicitările în creştere de acces la date. Chiar dacă majoritatea organizaţiilor din sectorul privat nu furnizează date contra cost, există şi unele care percep o taxă pentru un astfel de serviciu.

Multe firme mari au servicii însărcinate cu respectarea procedurilor penale care gestionează solicitările de date, însă îşi re-examinează periodic resursele pentru a se asigura că procedurile instituite sunt eficiente din punct de vedere al costurilor. Multe firme mici nu pot spera să repete acest gen de experienţă, iar acesta este un aspect care trebuie avut în vedere atunci când se analizează posibilitatea de a solicita date. Autorităţile publice par să nu îşi fi organizat resursele astfel încât să reflecte sectorul privat. Procurorii şi/ sau ofiţerii organelor de aplicare a legii au dreptul să emită solicitări de date în cursul anchetelor desfăşurate, însă există motive întemeiate să se afirme că, pentru ca aceste solicitări să aibă mai multe şanse să fie încununate de succes, trebuie să fie filtrate printr-un birou cunoscut şi sub denumirea de Punct unic de contact (SPoC), unde li se face controlul calităţii şi sunt prioritizate înainte să fie trimise sectorului privat.

Sectorul privat apoi va avea de-a face doar cu SpoC şi nu cu cel însărcinat cu desfăşurarea urmăririi penale, şi va transmite toate informaţiile sau datele direct către SpoC pentru ca acesta să le disemineze ulterior. Personalul care lucrează la SpoC beneficiază de pregătire specială pentru a se ocupa de solicitările de date. Utilizând această instituţie, personalul SpoC devine expert în acest domeniu de activitate şi acţionează ca un punct excelent de referinţă pentru cooperarea cu sectorul privat, punându-se la curent în permanenţă cu progresele tehnice.

Punctul unic de contact (SPoC) şi pentru furnizorii de servicii (servicii însărcinate cu respectarea procedurilor penale în cazul sectorului privat) şi pentru organele de aplicare a legii reprezintă un aspect esenţial al reuşitei. În acest context, punctul unic de contact este fie o persoană acreditată, fie un grup de persoane acreditate, pregătite să faciliteze dobândirea licită de date de comunicaţii şi cooperarea efectivă dintre o autoritate publică şi furnizorii de servicii. Pentru a fi acreditată, persoana finalizează un curs de formare profesională adecvată pentru rolul din cadrul unui SpoC, după care i se va încredinţa un Cod personal de identificare SPoC (PIN). Informaţiile privind toate persoanele acreditate le sunt disponibile şi furnizorilor de servicii, pentru scopuri de autentificare.

Pentru a sprijini în plus rata de succes în obţinerea datelor deţinute de societăţi comerciale private, formularele standardizate de solicitare transmise de organele de aplicare a legii sectorului privat şi viceversa ar putea facilita şi îmbunătăţi rezultatele din anchetă. Respectivele formulare, create pe baza contribuţiilor procurorilor şi a personalului organelor de aplicare a legii din România, Bulgaria şi Ungaria, împreună cu cele ale furnizorilor de servicii şi ale sectorului financiar, validate într-un cadru mai cuprinzător, ar putea fi adaptate unui număr mai mare de jurisdicţii, astfel încât să beneficieze şi alte State Membre UE dacă le vor folosi sau dacă îşi vor adapta versiunile respective.

Prezentul proiect cu finanţare CE a susţinut şi a sprijinit un nivel mai înalt al dialogului şi parteneriatelor pozitive dintre organele de aplicare a legii şi sectorul privat, în scopul identificării în comun a mijloacelor şi metodelor de cooperare pentru combaterea faptelor penale de pe internet. Proiectul recunoaşte contribuţiile valoroase ale furnizorilor de servicii de internet şi ale furnizorilor de servicii ale societății informaţionale în scopul combaterii infracţiunilor de pe internet şi nevoia de a construi un cadru de colaborare constructivă. Sectorul privat elaborează dinamic noi tehnologii, strângând şi

stocând în acelaşi timp date care sunt vitale pentru depistarea şi prevenirea infracţiunilor de pe internet, iar autorităţile de la nivel mondial adoptă noi legi pentru a ţine pasul cu provocările tehnologiei.

Cu cât se reunesc mai frecvent aceşti factori implicaţi pentru a soluţiona împreună aspectele de interes comun fără a îşi compromite responsabilităţile ce le incumbă prin lege, cu atât mai mari vor fi ocaziile de a îi aduce pe infractori în faţa justiţiei. Sectorul privat necesită pregătire pentru a înţelege natura în schimbare a cerinţelor juridice, iar procurorii şi reprezentanţii organelor de aplicare a legii trebuie să înţeleagă şi să identifice mijloacele necesare pentru a profita de serviciile tehnologice într-o continuă schimbare şi datele care le stau la dispoziţie. Încercarea de regularizare şi de standardizare a fluxului de informaţii dintre cele două sectoare nu are decât de profitat de pe urma rezultatului acţiunilor comune şi a colaborării.

Statistici ilustrative pentru ţările participante[1]

Statul	Populaţia	Utilizatori de internet (iunie 2010, ITU)	Accesul populaţiei la internet	Utilizatori de Facebook iunie 2011	Accesul populaţiei la Facebook
Bulgaria	7.093.635	3.395.000	47,9%	2.156.780	30,4%
Ungaria	9.976.062	6.176.400	61,9%	3.358.160	33,7%
România	21.904.551	7.786.700	35,5%	3.424.100	15,6%
EU-27	502.748.071	338.469.075	67,3%	159.673.320	31,8%

În plus faţă de paşii detaliaţi pentru cooperare, evidenţiaţi în capitolul „Paşi în sensul cooperării”, prezentul manual include (Anexa VII – Formular de solicitare a datelor de trafic)

[1] www.internetworldstats.com/europa.htm (accesat ultima oară la 1 decembrie 2011)

formularul structurat care a fost creat pentru schimbul de date, proiectat special pentru cele trei tipuri diferite de organizaţii

- Furnizor de Servicii Electronice
- Furnizor de Telecomunicaţii
- Instituţie Financiară

Mulţumiri

Multe entităţi au contribuit la acest proiect. Se cuvin mulţumiri speciale personalului Serviciul de Parchet al Coroanei (Marea Britanie), Agenţiei de Combatere a Infracţiunilor Grave şi de Crimă Organizată (Marea Britanie), Interpol-ului, Serviciului de Poliţie Metropolitană (Marea Britanie) şi multor altor lucrători şi organe de aplicare a legii de pe glob.

Introducere

Proiectul actual

Prezentul manual vizează asigurarea eficienţei şi eficacităţii anchetării faptelor penale de pe internet prin regularizarea şi standardizarea fluxului de informaţii dintre agenţiile de aplicare a legii şi furnizorii de servicii de internet şi furnizorii de servicii ale societăţii informaţionale. Astfel, fluxul de date va fi mai rapid, iar informaţiile de la furnizorii de servicii vor fi prezentate procurorilor într-o formă adecvată pentru a servi drept probatoriul în cursul procedurilor din instanţă. Procesul va mai avea un impact pozitiv cu privire la stimularea asistenţei judiciare internaţionale în cazul solicitărilor privind strângerea de probe pentru infracţiunile online.

Coordonatorul proiectului, D-na Ioana Albani are masteratul în drept şi 12 ani de experienţă ca procuror de anchetă şi de şedinţă. În ultimii patru ani de zile, D-na Albani a fost şeful Unităţii de Criminalitate Informatică din cadrul Direcţiei pentru Investigarea Infracţiunilor de Crimă Organizată şi Terorism, iar anterior acestei funcţii a coordonat prima unitate specializată pe criminalitate informatică şi spălare de bani în cadrul Parchetului General al României. Mai deţine, de asemenea, şi cunoştinţe cuprinzătoare de management de proiect, deoarece între decembrie 2006 şi februarie 2008 a fost vice-coordonatorul unui proiect Phare – Combaterea criminalităţii organizate – cu o abordare inter-instituţională, cu sarcina de supraveghere a procesului de punere în practică a activităţilor din cadrul proiectului, de asigurare a legăturii cu experţii străini etc.

Prin intermediul cooperării directe şi al dialogului constructiv

dintre procurori, poliţie şi reprezentanţii furnizorilor de servicii de internet sau prin intermediul internetului, se va dezvolta cadrul pentru viitoarea asistenţă pentru urmărirea penală a infracţiunilor informatice, inclusiv retragerea conţinutului de pornografie infantilă. Au fost create formulare standardizate pentru schimbul de date (indiferent de jurisdicţie) dintre două categorii de factori implicaţi, susţinute de liniile directoare de cooperare, cu informaţii cu privire la gestionarea relaţiilor menţionate. Ca atare, rezultatul proiectului va fi benefic atât pentru procedurile judiciare naţionale cât şi pentru cele transfrontaliere.

Cadru general

Consiliul Europei

Atât organele de aplicare a legii, cât şi furnizorii de servicii de internet joacă un rol esenţial în ceea ce priveşte consolidarea încrederii în tehnologiile informaţionale şi de comunicaţii (ICT) şi ajută societăţile de pe glob să se servească cel mai bine de aceste tehnologii.

Deoarece urmărirea penală a criminalităţii informatice de către organele de aplicare a legii se dovedeşte adesea mai puţin eficientă şi eficace dacă nu există cooperare cu furnizorii de servicii de internet, este esenţial ca ambele entităţi să coopereze una cu cealaltă într-un mod eficient şi eficace din punctul de vedere al costurilor.

Rolurile ambelor sunt distincte şi trebuie respectate: organele de aplicare a legii anchetează şi depistează infracţiuni, iar furnizorii de servicii le oferă utilizatorilor de internet posibilitatea să comunice la nivel mondial.

Chestiunea cu care se confruntă multe ţări este cum pot să coopereze cel mai bine cele două sectoare, astfel încât internetul să devină mai sigur, respectându-se, în acelaşi timp, rolurile diferite şi drepturile fundamentale ale utilizatorilor.

O componentă esenţială a soluţiei – ba chiar mai mult decât atât, o condiţie preliminară a cooperării – o constituie prevederile legislative clare care definesc responsabilităţile, autorităţile şi limitele. În această privinţă este esenţială punerea deplină în practică a Convenţiei privind Criminalitatea Informatică, în special a prevederilor acesteia privind dreptul procedural.

Dezbaterile din mai multe ţări din întreaga lume au reliefat necesitatea unor linii directoare practice, care să sprijine organele de aplicare a legii şi furnizorii de servicii să îşi organizeze şi să îşi structureze cooperarea.

În 2007, în consecinţă, Consiliul Europei – în cadrul Proiectului privind Criminalitatea Informatică – a instituit un grup de lucru, cu reprezentanţi ai organelor de aplicare a legii, şi ai asociaţiilor de sector şi ale furnizorilor de servicii, care, la rândul lor, au redactat liniile directoare care au fost adoptate în cursul Global Octopus Interface Conference de la Strasbourg din aprilie 2008[2].

Declaraţia Consiliului UE privind rolul PPP

Cel de-al 2987-lea Consiliu pe Justiţie şi Afaceri Interne a declarat la reuniunea din noiembrie 2008[3] că în căutarea unui răspuns eficace la diferitele tipuri de ameninţări privind reţelele electronice, trebuie să se recurgă la măsuri orizontale precum consolidarea parteneriatului dintre autoritățile publice și sectorul privat în vederea elaborării în comun a unor metode de identificare și de prevenire a prejudiciilor cauzate de activitățile infracționale și în vederea comunicării din partea societăților victime către organismele de aplicare a legii a informațiilor relevante privind frecvența delictelor.

În special, se recomandă Comisiei să abordeze în detaliu orientările adoptate de Conferința pe tema cooperării globale privind combaterea criminalității informatice, desfășurată sub auspiciile Consiliului Europei în perioada 1-2 aprilie 2008, care a urmărit îmbunătățirea parteneriatului dintre autoritățile publice și sectorul privat în combaterea criminalității

[2] Anexa I

[3] Concluziile Consiliului privind o Strategie de Lucru Concertată şi Măsurile Concrete de Combatere a Criminalităţii Informatice de la reuniunea celui de-al 2987-lea Consiliu pe JUSTIŢIE şi AFACERI INTERNE de la Bruxelles, 27-28 noiembrie 2008

informatice. În acest context, Consiliul ia notă de recomandările făcute la încheierea reuniunii experților organizate de Comisie în perioada 25-26 septembrie 2008 a acestui an, redate în anexă;

Crearea unei platforme europene destinate semnalării infracțiunilor săvârșite prin intermediul internetului şi elaborarea, în consultare cu operatorii privați, a unui model european de cooperare între organele de aplicare a legii și operatorii privați;

În concluziile Consiliului Uniunii Europene (2009/C 62/05) din 27 noiembrie 2008 privind o strategie de lucru concertată şi măsuri concrete pentru combaterea criminalităţii informatice se afirmă că, Consiliul:

1. CONSIDERĂ că este important să fie combătute diferitele elemente ale criminalității informatice și invită statele membre și Comisia să definească o strategie de lucru concertată, ținând seama de conținutul Convenției Consiliului Europei privind criminalitatea informatică.
2. CONSIDERĂ că, în căutarea unui răspuns eficace la diferitele tipuri de amenințări privind rețelele electronice, trebuie să se recurgă la măsuri orizontale precum:

(a) consolidarea parteneriatului dintre autoritățile publice și sectorul privat în vederea elaborării în comun a unor metode de identificare și de prevenire a prejudiciilor cauzate de activitățile infracționale și în vederea comunicării din partea societăților-parte vătămată către organismele de aplicare a legii a informațiilor relevante privind frecvența delictelor. În special, se recomandă Comisiei să abordeze în detaliu orientările adoptate de Conferința pe tema cooperării globale privind combaterea criminalității informatice, desfășurată sub auspiciile Consiliului Europei în perioada 1-2 aprilie 2008, care a

urmărit îmbunătățirea parteneriatului dintre autoritățile publice și sectorul privat în combaterea criminalității informatice. În acest context, Consiliul ia notă de recomandările făcute la încheierea reuniunii experților organizate de Comisie în perioada 25-26 septembrie 2008 a acestui an, redate în anexă;

(b) îmbunătățirea cunoașterii reciproce și a formării în rândul actorilor angajați în combaterea criminalității informatice în Europa. În special, ar fi oportună formarea unei rețele a șefilor de servicii de combatere a criminalității informatice. Această inițiativă ar suplimenta, într-adevăr, lucrările întreprinse de către grupurile de experți active în domeniu, care vor avea în vedere nu numai riscurile viitoare, ci și procedurile pentru acțiuni urgente în caz de incidente majore, în mod similar grupului instituit sub auspiciile Europol, sau lucrările întreprinse de către centrele comune de cercetare instituite de Comisiei; INVITĂ, din acest punct de vedere, statele membre și Comisia să introducă măsuri bazate pe studii de caz, în special ținând seama de dezvoltările tehnologice, pentru elaborarea de instrumente destinate utilizării operaționale, pe termen scurt și mediu, precum şi:

(c) pe termen scurt: elaborarea, în consultare cu operatorii privați, a unui model european de cooperare între organele de aplicare a legii și operatorii privați,

DG Afaceri Interne

Proiectul

Pe pagina de internet a DG Afaceri Interne[4] se afirmă că programul general „Securitate și protecția libertăților” şi

[4] http://ec.europa.eu/home-affairs/funding/isec/funding_isec_en.htm (accesat ultima oară la 2 decembrie 2011)

programul specific „Prevenirea şi combaterea infracționalității" (Programul ISEC[5]) (600 de milioane Euro pentru perioada 2007–13) contribuie la securitatea cetățenilor prin prevenirea şi combaterea criminalităţii, în special a terorismului, traficului de persoane, abuzului de minori, a criminalităţii informatice, a traficului de droguri ilegale şi de arme, a corupţiei şi a fraudei. Se concentrează pe patru tematici:

- prevenirea criminalităţii
- aplicarea legii
- protecția şi sprijinirea martorilor
- protecția victimelor.

Se oferă sprijin financiar pentru acţiuni care vizează sporirea cooperării operative (de exemplu, consolidarea relaţionării, a încrederii şi înţelegerii reciproce, a schimburilor şi a diseminării de informaţii, experienţe şi bune practici), activităţile de monitorizare şi evaluare, dezvoltarea şi transferul de tehnologie şi metodologie, formarea şi schimburile de personal, precum şi consolidarea nivelului de conştientizare şi activităţi de diseminare. Printre priorităţile din 2010 se numără **Utilizarea ilegală a internetului**: susţinerea cooperării dintre experţi şi autorităţile de aplicare a legii cu privire la înţelegerea şi combaterea fraudelor şi a comerţului ilegal de pe internet; acţiuni vizând instituirea de formulare standardizate pentru solicitările organelor de aplicare a legii către sectorul privat şi viceversa; acţiuni împotriva conţinutului ilegal care poate incita minorii la comportamente violente şi alte tipuri de comportamente grave; cooperarea pentru elaborarea şi schimbul de metode eficiente de monitorizare a internetului pentru identificarea şi combaterea conţinutului terorist.

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:058:0007:0012:EN:PDF

Toate iniţiativele trebuie să contribuie la realizarea obiectivelor Programului. Printre elaborarea eficientă şi eficace, punerea în practică, monitorizarea şi evaluarea instrumentelor şi a politicilor Uniunii Europene se includ:

- schimbul, diseminarea şi utilizarea informaţiilor, a cunoştinţelor, experienţei şi a celor mai bune practici între Statele Membre;
- dezvoltarea cooperării dintre actorii relevanţi de securitate şi furnizarea de strategii, tehnici şi instrumente pentru ca aceştia să îşi îmbunătăţească rezultatele legate de prevenirea şi combaterea criminalităţii;
- dezvoltarea coordonării şi consolidarea înţelegerii reciproce la nivelul autorităţilor de aplicare a legii, facilitarea coordonării activităţilor acestora, precum şi consolidarea capacităţii acestora de a combate criminalitatea şi activitatea teroristă, în special în dosare cu o dimensiune transfrontalieră;
- elaborarea de noi metode şi tehnici pentru susţinerea organelor operative de aplicare a legii şi pentru îmbunătăţirea pregătirii şi a capacităţii de a le aplica, inclusiv analizarea modului în care se pot folosi noile tehnologii pentru scopurile organelor de aplicare a legii;
- promovarea parteneriatelor public-privat între organele de aplicare a legii care iau măsuri pentru prevenirea criminalităţii şi a atentatelor teroriste;

Metodologia proiectului

Prezentare generală

Durata totală a prezentului proiect este de douăsprezece luni. Cele două ateliere de câte patru zile fiecare au oferit posibilitatea dialogului şi a parteneriatului dintre procurori, organele de aplicare a legii şi sectorul privat în vederea identificării mijloacelor comune de cooperare pentru combaterea infracţiunilor de pe internet. La fiecare dintre ateliere a participat un număr total de şaisprezece procurori, ofiţeri de poliţie şi reprezentanţi ai furnizorilor de servicii de internet şi de societate informaţională din România, Bulgaria şi Ungaria.

În septembrie 2011 au fost recrutaţi doi experţi – dl. Cormac Callanan şi dl. Peter Robbins. Rolul experţilor a fost să coordoneze şi să faciliteze implementarea celor două ateliere din Sofia (activitatea nr. 2 din cadrul proiectului) şi Budapesta (activitatea nr. 3) şi o reuniune de tip masă rotundă în Bucureşti (activitatea nr. 5). Ulterior, experţii au propus măsuri referitoare la modul în care s-ar putea consolida dialogul dintre sectoarele public şi privat şi au produs un set de formulare pentru standardizarea solicitărilor făcute de agenţiile de aplicare a legii către companiile de internet şi instituţiile financiare pentru datele deţinute, pentru a îi sprijini în investigarea şi urmărirea penală a faptelor penale comise pe internet.

Între septembrie 2011 şi decembrie 2011, cei doi experţi au cercetat şi au colaţionat informaţiile generate prin intermediul reţelelor lor de contacte globale şi au trecut în revistă materialele publicate relevante pentru a aduce un plus de

valoare la discuţiile dintre participanţii invitaţi din România, Bulgaria şi Ungaria. În strânsă cooperare cu managerul de proiect au fost proiectate şi structurate atelierele, astfel încât să analizeze domeniile de impact direct pentru scopurile proiectului, prin identificarea tematicilor esenţiale, ale experienţelor critice din sectoarele public şi privat şi prin intermediul prezentărilor esenţiale.

A devenit clar că multe organizaţii din sectorul privat care deţin date de comunicaţii îşi instituiseră deja proceduri şi procese sistematice de respectare a legislaţiei penale pentru a gestiona solicitările pentru servicii pe care le-ar putea primi. Situaţia era adevărată în special în cazul societăţilor multinaţionale care îşi proiectaseră procesele de activitate pentru a face faţă solicitărilor primite din partea organelor de aplicare a legii de peste tot din lume. Toate aveau protocoale scrise de urmat de către personalul propriu şi multe au pus la dispoziţie linii directoare către organele de aplicare a legii în care specificau gama de servicii pe care o pot furniza, împreună cu perioadele în care păstrează datele şi note explicative cu privire la modul în care trebuie interpretate datele furnizate. Evident, viteza de dezvoltare şi produsele noilor tehnologii reprezintă o adevărată provocare pentru sectorul privat în sensul canalizării informaţiilor actualizate către organismele relevante din sectorul public, însă mulţi dintre vorbitorii reprezentând sectorul privat au făcut dovada dorinţei lor de a se implica şi de a partaja experienţe pentru a garanta cel mai eficient rezultat pentru toţi cei interesaţi.

După re-examinarea diferitelor formulare de solicitare de date diferite din România, Bulgaria, Ungaria, Marea Britanie, Germania, Noua Zeelandă şi Canada, a reieşit clar că majoritatea acestor formulare de solicitare erau minimaliste prin scopul urmărit, însă puteau fi utilizate susţinut la nivel regional şi internaţional de către sectorul privat, chiar dacă stilurile, formatele şi criteriile referitoare la informaţii nu corespundeau întotdeauna.

Produsul discuţiilor din cadrul atelierelor a fost reprezentat de liniile directoare scrise pentru cooperarea dintre cele două categorii de actori, precum şi de propunerile de formulare standardizate pentru solicitările făcute de organele de aplicare a legii către sectorul privat. Au fost, de asemenea, dezbătute aspectele referitoare la cooperarea transfrontalieră privind investigarea infracţiunilor de criminalitate informatică.

Liniile directoare (activitatea nr. 4) şi formularele standardizate vizează sprijinul pentru îmbunătăţirea eficienţei şi eficacităţii investigaţiei infracţiunilor comise pe internet prin regularizarea şi standardizarea fluxului de informaţii dintre organele de aplicare a legii şi furnizorii de servicii de internet/ societate informaţională. S-a inclus şi un exemplu de înştiinţare de blocare a conţinutului pornografic infantil ilegal de pe internet.

Cele două ateliere au avut loc:

- primul la Sofia în septembrie 2011[6].
- cel de-al doilea la Budapesta în noiembrie 2011[7].

Masa rotundă finală a fost organizată la Bucureşti în decembrie 2011[8].

În scopul validării liniilor directoare scrise şi a formularelor standardizate, evenimentul final, masa rotundă, organizat la Bucureşti, a inclus experţi din Statele Membre din Europa Centrală şi de Est (un reprezentant al organelor de aplicare a legii sau un reprezentant al unui furnizor de servicii de internet/ societate informaţională pentru fiecare stat). Această reuniune a avut rolul de mijloc de diseminare a rezultatelor proiectului.

Versiunea finală a liniilor directoare şi a formularelor

[6] Consultaţi anexa II pentru lista participanţilor şi ordinea de zi
[7] Consultaţi anexa III pentru lista participanţilor şi ordinea de zi
[8] Consultaţi anexa IV pentru lista participanţilor şi ordinea de zi

standardizate produse în limba engleză a fost furnizată pe un suport de DVD/ CD şi diseminată organizaţiilor partenere din toate Statele Membre ale UE, pentru a servi drept model de cooperare dintre organismele de cercetare şi de urmărire penală şi sectorul privat din domeniu.

Prezentarea pe scurt a atelierelor

Atelierele de la Sofia, Budapesta şi Bucureşti

Timp de opt zile au fost organizate ateliere (27 – 30 septembrie şi 15 – 18 noiembrie) la care au participat cel puţin şaisprezece procurori, ofiţeri de poliţie, şi diferiţi furnizori de internet din Ungaria, România şi Bulgaria, împreună cu furnizorii de servicii internaţionale. Sectorul privat a făcut demonstraţii cu şi şi-a descris diferitele servicii pe care le furnizează, a explicat tipurile de date pe care le deţin care pot fi relevante pentru anchetele penale, câtă vreme sunt păstrate aceste date, care sunt dificultăţile pe care le au atunci când se confruntă cu multe solicitări din partea OAL şi/ sau a Procurorilor, cum s-ar putea îmbunătăţi relaţiile şi dacă formularul standardizat de solicitare din partea Autorităţilor ar eficientiza prelucrarea solicitărilor.

Contribuţiile din Bulgaria

- Prezentarea generală a instrumentelor internaţionale relevante, inclusiv pornografia infantilă, legislaţia privind păstrarea datelor şi diferitele tipuri de cooperare din cele trei ţări participante
- Evaluarea diferitelor cadre naţionale din România, Bulgaria şi Ungaria.
- Prezentări privind cadrele juridice naţionale privind protecţia datelor cu caracter personal/ privat
- Exemple naţionale/ internaţionale de schimburi de informaţii dintre organele de aplicare a legii

- Exemple naţionale/ internaţionale de probleme cu probatoriul în cursul executării solicitărilor din străinătate
- Soluţionarea dosarelor de pornografie infantilă atunci când sunt prezente diferite canale de distribuţie
- Cadrele juridice cu privire la sectorul bancar
- Cadrele juridice referitoare la legile relevante privind telecomunicaţiile
- Metodologiile de anchetă ale organelor de aplicare a legii şi probleme privind strângerea probatoriului
- Discuţii privind creşterea numărului de infracţiuni informatice cu exemple de arestări şi urmăriri penale reuşite
- O informare substanţială cu privire la Liniile Directoare ale Consiliului Europei privind cooperarea dintre organele de aplicare a legii şi furnizorii de servicii de internet împotriva criminalităţii informatice

Contribuţiile din Ungaria

- Prezentarea Biroului Naţional de Investigaţii, Unitatea de Combatere a Criminalităţii Informatice referitoare la fraudele cu carduri de credit şi informaţii privind dosarele investigate referitoare la infracţiuni grave de criminalitate informatică. S-au inclus aici exemple de partajare de informaţii cu sectorul privat.

- Prezentarea Microsoft Ungaria care a explicat noul program de calculator care îi identifică pe minorii exploataţi sexual, iar delegaţiei i s-a spus cum îşi organizează compania resursele la nivel global pentru a gestiona solicitările privind date de acces primite din partea organismelor publice de la nivel mondial.

- Furnizorii de comerţ electronic – prezentarea paginii de internet de comerţ electronic Vatera. Am aflat că şi-au dezvoltat propriile linii directoare interne pentru cooperare cu organele de aplicare a legii.

- Furnizorii de telecomunicaţii – Vodafone Ungaria şi România, împreună cu Hungarian Telecom şi-au explicat metodele prin care strâng şi prezintă datele, inclusiv sistemele de percheziţie electronică şi recuperare a datelor, pentru a răspunde la solicitările de date. A fost reprezentată şi firma Telenor.

- Asociaţia Băncilor din Ungaria şi-a prezentat problemele legate de relaţia pe care o au cu organele de aplicare a legii.

- Reprezentantul Interpol a explicat rolul şi mandatul instituţiei şi a comentat cu privire la cooperarea poliţienească internaţională şi provocările conexe.

- Parchetul General al Ungariei şi-a demonstrat proiectul de implementare a unui sistem electronic de prelucrare a dosarelor. Cu ajutorul acestui sistem are posibilitatea de a transmite şi primi toate documentele prin intermediul unei reţele informatice pe baza certificatelor electronice. Această prezentare s-a mai raportat şi la aspectele de asistenţă judiciară internaţională.

- Reprezentantul echipei maghiare de reacţie în situaţii de urgenţă informatică a explicat rolul şi funcţia instituţiei sale care şi-a consolidat relaţii formale şi informale bune cu sectorul privat şi la nivel naţional, dar şi cu omologii din străinătate. Vorbitorul a explicat modul de acţiune urgent al instituţiei pentru a bloca adresele de IP din afara Ungariei dacă sunt folosite cu reaua intenţie de a bloca sistemele bancare prin internet (de exemplu, în cazul unui atac distribuit DOS) şi ce face aceasta

pentru a combate atacurile de phishing prin sistemele de notificări şi blocare. Organismele CERT de la nivel naţional păstrează şi strâng informaţiile privind adresele de IP ale calculatoarelor zombie, potenţial infectate pentru a face parte din reţele botnet.

- Reprezentantul reţelei sociale Facebook a explicat scala şi complexitatea serviciilor proprii şi problemele pe care le au în ceea ce priveşte gestionarea numărului mare de solicitări de date de peste tot de pe glob.

- Asociaţia pentru protecţia drepturilor de autor (Asociaţia PROART) a explicat cum cooperează cu parchetele şi autorităţile de anchetă în cazul infracţiunilor de proprietate intelectuală care cad în sarcina instituţiei.

Contribuţiile din România

- Participanţilor şi experţilor li s-au alăturat reprezentanţi ai altor cinci state din UE, Slovenia, Republica Cehă, Lituania, Austria şi Republica Slovacă. Au participat reprezentanţi ai Vodafone şi Microsoft România, împreună cu reprezentanţii Asociaţiei Furnizorilor de Servicii de Internet din România şi ai Asociaţiei Băncilor din România.

- Prezentarea paşilor practici care îi pot sprijini pe reprezentanţii sectoarelor publice şi private să iniţieze dialogul constructiv, şi au fost analizate câteva exemple de acţiune în parteneriat din alte regiuni. Delegaţii au mai discutat şi modificat un şablon pentru a putea fi folosit ca formular standardizat de solicitare. Atelierul s-a încheiat cu angajamentul pozitiv al celor prezenţi de a exersa folosirea liniilor directoare şi a formularelor standardizate.

Probleme identificate

Mai mulţi vorbitori şi participanţi au putut să partajeze exemple de rezultate pozitive, deoarece buna voinţă, solicitările personalizate, cooperarea de primă mână, inclusiv protocoalele scrise dintre sectoarele public şi privat au condus în final la arestări şi urmăriri penale reuşite. Cu toate acestea, trebuie trase învăţăminte în urma discuţiilor legate de diferitele situaţii care nu au fost finalizate cu un rezultat pozitiv sau care au condus la respingeri dintr-o serie de motive, printre care se includ:-

- întârzieri nedorite din cauza problemelor de interpretare
- neînţelegeri privind gama şi nivelul de servicii a furnizorilor
- nefamiliarizarea cu tehnologiile folosite la comiterea infracţiunii
- solicitări disproporţionate de date
- dacă nu se făcea solicitarea de urgenţă nu erau incluşi indicatori ai priorităţii
- solicitări de păstrare care n-au fost monitorizate ulterior
- stabilirea de calendare nerezonabile
- datele nu au fost solicitate de o manieră suficient de detaliată
- detalii insuficiente cu privire la profilul bănuiţilor
- informaţii inadecvate privind verificarea şi validarea primite din partea solicitanţilor
- dovezi puţine sau deloc cu privire la măsurile de control al calităţii
- sisteme juridice incompatibile
- expirarea perioadelor de păstrare a datelor
- solicitări neautorizate sau neverificate

- lipsa de cunoştinţe cu privire la complexitatea platformelor IT şi interoperabilitatea serviciilor la nivelul furnizorilor de servicii
- solicitări vagi sau imprecise
- lipsa ocaziilor de a împărtăşi şi face schimb de experienţă
- cunoştinţe/ pregătirea insuficiente ale personalului pentru a optimiza solicitările
- feedback insuficient atunci când eşuează o solicitare
- lipsa dorinţei de a recompensa furnizorul de servicii pentru cheltuielile ocazionate de recuperarea datelor
- solicitările pe hârtie sunt înlocuite treptat de mijloacele electronice, însă sunt necesare colaborarea şi pregătirea suplimentare
- recunoaşterea faptului că solicitările trebuie să fie marcate drept confidenţiale dacă nu trebuie să fie informat abonatul în această privinţă

Concluziile experţilor

Experţii au fost de părere că aceste probleme ar fi cel mai bine rezolvate prin crearea funcţiei unui Punct Unic de Contact (SPOC) în cadrul autorităţilor publice şi adoptarea unui set de formulare standardizate de solicitări de date.

Experienţe internaţionale

Irlanda

În 1998 a fost înfiinţat Comitetul privind utilizarea ilegală şi nocivă a internetului[9] pentru a examina utilizarea ilegală şi nocivă a acestuia. Internetul face atât de mult rău cât face şi bine. De fapt, se poate susţine că, datorită anonimatului relativ şi a dimensiunilor globale, internetul facilitează cel mai bine exprimarea neîngrădită a laturii noastre ascunse prin comparaţie cu orice alt mijloc de comunicaţie existent în prezent. Pentru a înţelege cu adevărat ce putem face pentru a ne raporta la dezavantajele internetului, trebuie mai întâi să ne confruntăm şi să înţelegem natura internetului. Din aceste motive, prezentul Raport discută contextul general şi aspectele redând şi detalii înainte de a recomanda o abordare adecvată.

Fără a face apel la măsuri extreme, nedorite, de cenzură şi restricţii, care sunt în mod clar impracticabile, internetul va include întotdeauna utilizatori care reprezintă laturile întunecate ale societăţii noastre. În consecinţă, Grupul consideră că nu se pune problema de a garanta îndepărtarea tuturor materialelor ilegale şi nocive de pe internet sau de a garanta imposibilitatea accesării acestor materiale. Se pune problema, mai degrabă, de a lua măsuri astfel încât internetul să devină un mediu sigur pentru utilizatorii săi, care ne va proteja copiii şi ne va respecta viaţa personală şi demnitatea cetăţenilor. Un astfel de mediu, credem noi, va fi creat pe baza iniţiativelor practice naţionale, a cooperării internaţionale intensive şi a unei creşteri a nivelului de conştientizare şi

[9] http://www.justice.ie/en/JELR/Pages/Illegal_use_of_the_Internet_report (accesată ultima oară la 15 decembrie 2011)

înţelegere a tuturor eşaloanelor societăţii cu privire la acest fenomen. Astfel de măsuri reprezintă coloana vertebrală a recomandărilor incluse în prezentul Raport.

Prezentul raport a identificat fenomenul internaţional al internetului, prin intermediul căruia, „din cauza naturii fundamentale a internetului, există limitări serioase cu privire la ce poate face o singură ţară pentru a soluţiona dezavantajele acestuia. Internetul ca atare este un fenomen internaţional în toată puterea cuvântului şi orice reacţie eficientă va trebui să se sprijine pe niveluri înalte de cooperare internaţională".

A propus o serie de măsuri care au fost implementate în Irlanda. Pachetul de măsuri strategice s-a concentrat pe patru domenii principale:

- introducerea unui sistem de auto-reglementare a sectorului de furnizori de servicii de internet, pentru a include coduri comune de practici (COPs) şi condiţii de utilizare acceptabile împărtăşite (AUCs)
- înfiinţarea unei linii verzi pe internet pentru a prelua, investiga şi prelucra plângerile legate de materialul ilegal de pe internet
- înfiinţarea unui Organism Consultativ pe Internet, care să coordoneze diferitele măsuri, pentru a asigura un mediu sigur pe internet, împreună cu un cadru de auto-reglementare
- elaborarea de programe de conştientizare pentru utilizatori, astfel încât aceştia să fie responsabilizaţi să se protejeze, sau să îi protejeze pe cei pe care îi au în grijă, faţă de materialele ilegale şi nocive de pe internet

Auto-reglementare

Aceasta este o componentă fundamentală şi esenţială a strategiei naţionale de reacţie la dezavantajele internetului şi trebuie vizată cu precădere. Auto-reglementarea prin

intermediul furnizorilor de servicii ar trebui să includă elaborarea de coduri de practici, care să se concentreze pe:

- promovarea unei conştientizări generale cu privire la aspectele de siguranţă de pe internet
- instituirea unei abordări comune legate de facilităţile de filtrare a conţinutului care pot fi puse la dispoziţia utilizatorilor individuali
- definirea procedurilor de interacţiune cu ceilalţi actori din mediul de auto-reglementare
- instituirea de proceduri pentru a garanta respectarea regulilor

Asociaţia Furnizorilor de Servicii de Internet din Irlanda[10] a fost înfiinţată în ianuarie 1998 de către Furnizorii Irlandezi de Servicii de Internet, activi pe piaţă la momentul respectiv. De atunci a fost susţinută şi de ISP-urile naţionale, dar şi de cele multinaţionale care au penetrat piaţa irlandeză. În prezent, numără 22 de membri care înseamnă furnizori de acces la internet şi de servicii de hosting.

Scopul asociaţiei este să reprezinte o singură voce a sectorului irlandez ISP la nivelurile naţional, al UE şi internaţional. Asociaţia este reprezentată în cadrul multor iniţiative guvernamentale şi oferă un punct public de contact pentru mass-media.

Este membru activ al EuroISPA, care reprezintă interesele a peste 500 ISP-uri europene la nivelul european. Se includ aici activităţi de lobby în parlamentul şi comisia europene în legătură cu setul actual de directive referitoare la internetul UE, cum ar fi păstrarea datelor, serviciul de mass-media audio-vizual (actualizarea TVwF), drepturile electronice de autor şi comerţul electronic etc.

[10] www.ispai.ie (accesată ultima oară la 15 decembrie 2011)

ISPAI a convenit împreună cu guvernul irlandez că abordarea de auto-reglementare a sectorului are şanse mai mari de reuşită şi de eficienţă. În consecinţă, ISPAI a înfiinţat serviciul www.hotline.ie pentru combaterea conţinutului ilegal, în special a pornografiei infantile găzduite şi distribuite pe internet. Linia verde online este activă din noiembrie 1999. În plus, au fost adoptate un cod de practici şi o politică de utilizare acceptabilă comune. ISP-urile convin să adere la acestea în momentul în care devin membri ai ISPAI.

Serviciul Hotline.ie al ISPAI[11] a fost lansat în noiembrie 1999 pentru a pune la dispoziţie un serviciu de raportare anonim pentru publicul care descoperă accidental conţinut ilegal pe internet, în special pornografie infantilă sau activităţi legate de exploatarea sexuală a minorilor. Linia verde de pe internet este susţinută şi finanţată de Asociaţia Furnizorilor de Servicii de Internet din Irlanda (ISPAI), ai cărei membri sunt hotărâţi să ia măsurile ce se impun pentru a combate utilizarea facilităţilor oferite de internet în astfel de scopuri ilegale.

Biroul pentru Siguranţa Internetului (OIS)[12] este un Birou Executiv al Ministerului Justiţiei şi Egalităţii. Biroul pentru Siguranţa Internetului (OIS) a fost înfiinţat de guvernul irlandez pentru a prelua principala responsabilitate legată de siguranţa pe internet în Irlanda, în special siguranţa copiilor. Biroul pentru Siguranţa Internetului vizează consolidarea de legături şi coeziune între toate ministerele şi instituţiile pentru a se asigura că Statul oferă cea mai bună protecţie posibilă pentru comunitate şi că promovează siguranţa pe internet, în special cu privire la combaterea pornografiei infantile.

Biroul pentru Siguranţa Internetului (OIS) consolidează şi supraveghează cadrul actual de auto-reglementare care a fost instituit de Asociaţia Furnizorilor de Servicii de Internet din

[11] www.hotline.ie (accesată ultima oară la 15 decembrie 2011)
[12] www.internetsafety.ie (accesată ultima oară la 15 decembrie 2011)

Irlanda (ISPAI).

Pentru a îşi îndeplini activitatea, Biroul pentru Siguranţa Internetului este susţinut de un Consiliu Consultativ pentru Siguranţa Internetului, ai cărui membri reprezintă factorii implicaţi din sectoarele legislativ, comercial şi comunitate.

Care îi vor fi responsabilităţile?

În calitate de organism consultativ primar, Consiliul Consultativ pentru Siguranţa Internetului va avea următoarele responsabilităţi

1. Să consilieze OIS cu privire la toate aspectele legate de siguranţa internetului, în special cele referitoare la copii
2. Să contribuie la monitorizarea şi implementarea deciziilor UE şi ONU referitoare la siguranţa internetului
3. Să contribuie la monitorizarea şi evaluarea cadrului de auto-reglementare pentru a asigura un mediu online mai sigur
4. Să ofere consiliere referitoare la priorităţile de cercetare din domeniu
5. Să ofere consiliere referitoare la creşterea nivelului de conştientizare în ceea ce priveşte utilizarea ilegală şi nocivă a internetului
6. Să ofere consiliere cu privire la elaborarea de mecanisme pentru a îi implica pe actorii esenţiali
7. Să examineze şi să evalueze abordările actuale de la nivelurile naţional şi internaţional pentru a soluţiona problema utilizării ilegale şi nocive a internetului

Consiliul consultativ are şi un subcomitet care răspunde de cooperarea dintre Organele de Aplicare a Legii şi Furnizorii de Servicii de Internet, iar acest comitet a elaborat un formular pentru schimbul de date dintre organele de aplicare a legii şi

furnizorii de servicii de internet în cursul cercetărilor penale.

Marea Britanie

În Marea Britanie li se permite prin lege mai multor autorităţi publice să solicite date de la Furnizorii de Servicii. Guvernul britanic a elaborat un Cod de Practici pentru Dobândirea şi Dezvăluirea Datelor de Comunicaţii în consultare cu sectorul privat. Codul stabileşte structura de cooperare dintre diferitele părţi implicate şi defineşte trei tipuri de date de comunicaţii. Codul mai stipulează şi cele patru funcţii ale persoanelor din cadrul autorităţilor publice pentru a se asigura că datele sunt prelucrate proporţional şi legal.

Datele de trafic se definesc drept:

- informaţii care identifică originea sau destinaţia unei comunicaţii care este, sau care a fost transmisă (inclusiv datele apelurilor primite);
- informaţii care identifică localizarea echipamentului atunci când comunicaţia este, a fost sau poate fi efectuată sau primită (cum ar fi localizarea unui telefon mobil);
- informaţii care identifică emiţătorul sau receptorul (inclusiv receptorii multipli) ai unei comunicaţii pe baza datelor incluse sau alăturate comunicaţiei;
- informaţii de rutare care identifică echipamentul prin intermediul căruia este sau a fost transmisă comunicaţia (de exemplu, alocarea unei adrese dinamice de IP, log-urile de transfer de fişiere şi şapourile de e-mail – în măsura în care conţinutul comunicaţiei, cum ar fi rândul de subiect dintr-un e-mail, nu este cunoscut);
- informaţia de navigare pe internet, în măsura în care doar un server de hosting, un server, numele de domeniu sau adresa de IP sunt cunoscute;

Informaţiile privind Utilizarea Serviciului se definesc drept:

- datele ordonate ale apelurilor telefonice (numerele apelate)
- datele ordonate ale conectărilor la servicii de internet;
- ora şi durata utilizării serviciului, într-un mod ordonat (apeluri şi/ sau conectări);
- informaţii referitoare la volumele de date descărcate şi/ sau încărcate;
- facturi ordonate care pot include indicarea costului pentru comunicaţiile primite, de exemplu, apeluri şi mesaje primite de un telefon mobil care a fost în „roaming" într-o altă reţea.
- informaţii privind utilizarea serviciilor care îi sunt alocate utilizatorului sau la care s-a abonat (sau e posibil să se fi abonat), inclusiv servicii de telecomunicaţii pentru apelurile în conferinţă, mesageria vocală, apeluri în aşteptare şi apeluri blocate;
- informaţii privind utilizarea serviciilor de forwarding/ redirecţionare;
- informaţii privind alegerea numerelor preferenţiale sau favorite;

Informaţiile privind abonatul se definesc drept:

- „verificări ale abonatului" (cunoscute şi sub numele de „căutări inversate") cum ar fi „cine este abonatul numărului de telefon 012 345 6789?", „cine deţine contul de e-mail example@example.co.uk?" sau „cine are dreptul să posteze pe spaţiul de pe internet *www.example.co.uk*?";
- informaţii despre contul abonaţilor sau al deţinătorilor de conturi, inclusiv numele şi adresele de la instalare,

precum şi facturarea, inclusiv metoda (metodele) de plată şi detaliile plăţilor;

- informaţii privind conectarea, deconectarea şi reconectarea la serviciile care îi sunt alocate abonatului sau deţinătorului contului, sau la care acesta s-a abonat (sau e posibil să se fi abonat), inclusiv servicii de telecomunicaţii pentru apelurile în conferinţă, mesageria vocală, apeluri în aşteptare şi apeluri blocate;
- informaţii privind aparatul utilizat sau pus la dispoziţia abonatului sau a deţinătorului contului, inclusiv producătorul, modelul, numerele de serie şi codurile aparatului;
- informaţii furnizate de un abonat sau de un deţinător de cont unui CSP, cum ar fi informaţii demografice sau date pentru crearea contului.

Roluri stipulate în ceea ce priveşte dobândirea de date

Solicitantul

a) Solicitantul este persoana implicată în desfăşurarea unei investigaţii sau operaţii pentru o autoritate publică relevantă, care face o solicitare scrisă sau electronică pentru dobândirea datelor de comunicaţii. Solicitantul completează un formular de solicitare, în care oferă, spre analiza persoanei desemnate, necesitatea şi proporţionalitatea unei cerinţe specifice privind dobândirea datelor de comunicaţii.

Persoana desemnată

a) Persoana desemnată este persoana cu o funcţie specificată în cadrul autorităţii publice relevante, care analizează cererea şi îşi specifică concluziile în scris sau electronic. Dacă persoana desemnată consideră că este necesar şi proporţional în circumstanţele specifice, se acordă autorizaţia sau se face înştiinţarea.

Punctul Unic de Contact (SPoC)

a) Punctul unic de contact este fie o persoană acreditată, fie un grup de persoane acreditate, pregătite să faciliteze dobândirea legitimă de date de comunicaţii şi cooperarea eficientă dintre o autoritate publică şi CSP. Pentru a fi acreditată, persoana trebuie să finalizeze un curs de formare adecvat pentru rolul unui SPoC şi să primească un Cod Personal de Identificare SPoC (PIN). Se pun la dispoziţia CSPs detaliile tuturor persoanelor acreditate pentru scopuri de autentificare.

Ofiţerul responsabil cu rang superior

a) integritatea procesului instituit în cadrul autorităţii publice pentru dobândirea datelor de comunicaţii;

b) respectarea legii şi a codului;

c) controlul raportării erorilor şi identificarea cauzelor erorilor, precum şi implementarea proceselor menite să diminueze şansele de repetare a erorilor;

d) implicarea, împreună cu organismul de control, atunci când acesta îşi desfăşoară inspecţiile, şi, dacă este necesar, controlul implementării planurilor de acţiune post-inspecţie.

Guvernul britanic a mai publicat, de asemenea, şi Liniile Directoare privind Asistenţa Judiciară Reciprocă

Aceste linii directoare se adresează entităţilor din străinătate şi se referă la modul în care acestea pot face o solicitare, însă, de fapt, toate solicitările de AJR trebuie transmise unei autorităţi centrale care le analizează.

Înainte de a face o cerere de AJR, li se sugerează autorităţilor din străinătate să facă uz de anchetele de la poliţie la poliţie sau de alte reţele de partajare de informaţii operative. Situaţia,

opinează ei, poate ajuta la îmbunătăţirea solicitării AJR şi la serviciile ulterioare care vor fi furnizate.

Li se cere autorităţilor solicitante să se asigure că solicitarea este proporţională (de exemplu, solicitarea de asistenţă este proporţională cu nivelul infracţiunii investigate), în special în cazul măsurilor intruzive sau care necesită timp (cum ar fi mandatele de percheziţie, filajul şi alte tipuri de asistenţă dispusă de instanţă). Forţele de poliţie din Marea Britanie sunt independente din punct de vedere operaţional şi prioritizează executarea cererilor de AJR în funcţie activitatea pe care o au de efectuat la nivel naţional. În consecinţă, şi date fiind resursele limitate disponibile organelor de aplicare a legii din Marea Britanie, e puţin probabil ca dosarele de minimis (solicitări pentru infracţiuni minore sau obişnuite) să aibă prioritate, li se solicită statelor solicitante să analizeze foarte bine necesitatea deţinerii probei respective. Se evaluează dosarele în integralitatea lor, însă în Marea Britanie e o situaţie obişnuită să se primească solicitări care sunt clar, de minimis, cum ar fi cele în legătură cu fraudele minore sau infracţiunile la Codul Rutier.

Se acordă prioritate solicitărilor care:

- Implică fapte penale deosebit de grave (de exemplu, omor sau alte fapte comise cu violenţă, crimă organizată, terorism, corupţie, sau fraudă pe scală largă)
- Implică probatoriu care poate fi ascuns sau distrus
- Implică infracţiuni în formă continuată sau care pun în pericol martorii sau societatea
- Implică o dată iminentă a procesului care trebuie să fie inclusă în Scrisoarea de Solicitare:
- Au antetul autorităţii emitente
- Sunt semnate de autoritatea emitentă

- Au o versiune tradusă în engleză, cu o copie pe hârtie semnată şi o altă copie

În cazul solicitărilor care nu sunt efectuate în limba engleză: o versiune pe hârtie, semnată, a solicitării în limba respectivă, şi o traducere în limba engleză a solicitării.

Trebuie incluse următoarele informaţii în conţinutul scrisorii:

1. detalii privind autoritatea care face solicitarea, inclusiv numele, numărul de telefon şi adresa de e-mail (dacă este disponibilă) a unei persoane de contact
2. scopul pentru care se solicită asistenţa
3. tipul de asistenţă care se solicită (de exemplu, dacă este o solicitare pentru strângere de probe, pentru trimiterea unei citaţii sau executarea unei dispoziţii de predare şi indisponibilizare etc.), precum şi orice alte informaţii suplimentare necesare pentru solicitări de acest tip de asistenţă
4. descrierea capetelor de acuzare sau pentru care se face cercetarea, precum şi sentinţa sau pedeapsa
5. copia legislaţiei care incriminează conduita respectivă în statul solicitant şi care oferă informaţii privind infracţiunea, pedeapsa, şi drepturile pe care le poate avea persoana cercetată.
6. rezumatul faptelor care au dat naştere solicitării şi legătura acestui dosar cu Marea Britanie
7. detalii referitoare la persoana sau persoanele (inclusiv numele legal) identificate în solicitare, inclusiv, dacă este disponibil, adresa, data naşterii şi naţionalitatea
8. detalii privind localizarea firmei/ persoanei de la care se solicită probe
9. dacă trebuie să i se facă o vizită unei persoane, să se specifice dacă este martor sau bănuit

10. numele bănuitului şi acuzaţiile care i se aduc.
11. legătura dintre probele solicitate şi infracţiunea cercetată/ proceduri. Trebuie stabilită o legătură directă clară între faptele de la dosar, după cum au fost detaliate în solicitare, şi probele solicitate. Asta înseamnă ceva mai mult decât să specifici pur şi simplu că materialul solicitat este relevant pentru dosar şi ar trebui specificat în ce mod este relevant şi va conduce la progrese în legătură cu dosarul
12. date relevante, cum ar fi data şedinţei de judecată (motivul urgenţei sau al atenţiei speciale ar trebui inclus pe foaia care prezintă scrisoarea de solicitare)
13. detalii, inclusiv numărul de telefon şi adresa de e-mail, dacă se cunoaşte, a oricărei agenţii sau a oricăror ofiţeri din organele de aplicare a legii din Marea Britanie, care sunt familiarizaţi cu ancheta (inclusiv, dacă este relevant, denumirea oricăror activităţi desfăşurate în Marea Britanie pe care le cunoaşte Statul Solicitant)
14. titlul Convenţiei relevante etc. în baza căreia se face solicitarea.
15. dacă aceasta este doar o solicitare pentru probe, specificaţi exact care sunt probele care sunt necesare (de exemplu, nu doar „evidenţe bancare", ci ce fel de tip de evidenţe bancare).
16. confidenţialitate – măsura în care se aplică confidenţialitatea

Studii de caz

În Marea Britanie, Serviciul de Poliţie Metropolitană are mii de ofiţeri de poliţie angajaţi. Oricare dintre aceşti ofiţeri are dreptul să facă o solicitare de date în cursul anchetelor pe care le desfăşoară, însă, pentru ca cererea să fie încununată de

succes, trebuie să fie aprobată de un ofiţer de rang superior, trebuie să fie înaintată unui birou central, cunoscut sub numele de Punct Unic de Contact (SPoC), care aprobă solicitarea, îi face controlul calităţii şi îi acordă un nivel de prioritate înainte de a o transmite sectorului privat.

După care, sectorul privat va avea de-a face doar cu SPoC şi nu cu ofiţerul care realizează ancheta, şi va transmite toate informaţiile sau datele direct SPoC pentru a le disemina mai departe. Personalul angajat la SPoC are pregătirea specială pentru a se ocupa de solicitările de date. Prin utilizarea acestei facilităţi, personalul SPoC a devenit expert în domeniu şi activează ca un punct excelent de referinţă pentru cooperarea cu sectorul privat, fiind în permanenţă la curent cu progresele tehnologice.

Ungaria şi România

În Ungaria şi în România, ofiţerii de poliţie şi procurorii au toţi dreptul de a face solicitări de date în cursul anchetelor pe care le desfăşoară. Înainte să fie transmise mai departe solicitările, sunt aprobate de şeful ofiţerului de poliţie sau al procurorului respectiv. În cazul solicitărilor transmise de ofiţerii de poliţie, acestea sunt frecvent verificate ulterior de procurorii care coordonează anchetele în curs. Reprezentanţii sectorului privat au de-a face direct cu autorităţile care le-au trimis solicitările.

Paşi în sensul cooperării

Esenţial pentru cooperarea dintre sectorul public şi privat este ca liderii de ambele părţi să iniţieze un dialog constructiv, dacă trebuie să îi protejeze împreună pe cetăţeni de criminalitatea informatică.

Linii Directoare privind Cooperarea dintre organele de aplicare a legii şi furnizorii de servicii.

Studiul cooperării dintre furnizorii de servicii şi organele de aplicare a legii împotriva criminalităţii informatice – în scopul celor mai bune linii directoare comune, create în 2009 de Consiliul Europei, se concentrează pe standardele internaţionale definite în Convenţia Consiliului Europei privind Criminalitatea Informatică (Budapesta, noiembrie 2001). Din cauza standardelor juridice naţionale diferite şi a lipsei unei analize detaliate de drept comparat în acest domeniu, a fost necesar să se elaboreze linii directoare privind respectarea legislaţiei penale la un nivel care să fie concret şi suficient de precis pentru a fi aplicabil pentru desfăşurarea de anchete pe de o parte, şi suficient de abstract ca să asigure că liniile directoare nu sunt in conflict cu standardele juridice existente. Liniile directoare mai pun la dispoziţie şi un cadru de cooperare împotriva criminalităţii informatice în general.

Analiza structurilor sistematice ale cooperării demonstrează că are o natură bidirecţională:

- Pe de o parte, organele de aplicare a legii sunt

răspunzătoare pentru prevenirea şi investigarea infracţiunilor, şi, pe de altă parte, sunt la curent cu tendinţele criminalităţii informatice.

- sectorul ICT este, pe de o parte, victima infracţionalităţii, şi, pe de altă parte, la curent cu câteva tendinţe ale criminalităţii informatice şi deţine date referitoare la clienţii care sunt făptuitorii sau victimele actelor infracţionale.

În general, sectorul de internet şi organele de aplicare a legii (OAL) recunosc interesul comun de prevenire, depistare şi investigare a criminalităţii informatice şi ameninţările la adresa securităţii naţionale şi a infrastructurii de informaţii în general. Siguranţa online, securitatea şi fiabilitatea internetului depind de depistarea timpurie a activităţii infracţionale, care poate submina realizarea acestor obiective. Cu toate acestea, în acest sens este necesară legislaţia efectivă care să echilibreze instrumentele de anchetă şi drepturile fundamentale cum ar fi dreptul persoanelor la intimitatea comunicaţiilor şi dreptul persoanelor să fie protejate de activităţile infracţionale.

Pe internet are loc o gamă largă de activităţi infracţionale, fiind postate inclusiv materiale cu abuzul ilegal de minori, discursuri pline de ură rasială, droguri online (se includ aici reţete, copii ilegale şi falsificate), pagini de internet cu cazinouri ilegale, precum şi abuzuri ilegale ale drepturilor de proprietate intelectuală.

Noile tipuri de infracţionalitate şi abuzul de tehnologie continuă să se dezvolte, incluzând abuzul de telefoane mobile (furtul de date personale şi filmuleţe stocate pe telefoanele mobile), pornografia generată pe calculator implicând adulţi şi minori, activităţi de „happy slapping”, cu folosirea telefoanelor mobile pentru a înregistra fapte penale săvârşite cu violenţă şi materiale pornografice cu copii create chiar de copii. Aceste noi tipuri de criminalitate creează provocări unice pentru organele de aplicare a legii şi pentru sectoarele tehnologiei informaţiilor şi a comunicaţiilor, din moment ce aceste produse şi servicii se

dezvoltă şi creează noi activităţi online, cum ar fi Group-On[13] sau Facebook[14] la nivelul cărora evoluează faptele penale multă vreme după ce a fost dezvoltat produsul. Noile produse şi servicii sunt mult mai mobile decât înainte şi au devenit dispozitive personale care sunt arareori partajate cu ceilalţi utilizatori şi nu mai sunt supravegheate de personalul pregătit în acest sens. Aceasta este o problemă extrem de complicată în special când vine vorba de supravegherea accesului minorilor la serviciile online. Desigur, nu este clar care sunt serviciile/ dispozitivele care vor avea succes şi nici care vor eşua şi este din ce în ce mai dificil să prognozezi care servicii vor atrage din ce în ce mai mulţi adepţi. Reprezintă o necunoscută specială care sunt noile riscuri individuale care se leagă de noile servicii şi dispozitive online. Celelalte domenii de provocări semnificative sunt cele ale criptării, ale virtualizării serviciilor şi cloud computing, care devin din ce în ce mai răspândite.

Crearea şi distribuţia de programe malware continuă, de asemenea, să evolueze. Peisajul ameninţării globale evoluează, iar programele malware şi cele nedorite potenţial devin din ce în ce mai regionale. Apar tipare extrem de diferite de ameninţări în diferite locuri de la nivelul global. Ecosistemul malware a depăşit stadiul ameninţărilor extrem de vizibile, cum erau viermii care se înmulţeau singuri, şi s-a îndreptat către ameninţări mai puţin vizibile care se bazează mai mult pe ingineria socială. În ultimii câţiva ani am fost martorii noilor tipuri de atacuri asupra sistemelor SCADA (sistemele de control al supravegherii şi de achiziţie de date) prin intermediul viermelui Stuxnet. Răspândirea şi eficacitatea programelor malware au devenit, de asemenea, mai dependente de limbaj şi de factorii culturali. Se răspândesc anumite ameninţări cu ajutorul tehnicilor care îi ţintesc pe cei care vorbesc o anumită limbă sau care folosesc servicii care sunt locale pentru o

[13] www.groupon.com
[14] www.facebook.com

anumită regiune geografică. Alte tipuri de malware iau în obiectiv vulnerabilităţi sau configuraţii şi aplicaţii ale sistemelor de operare cu distribuţie inegală la nivelul mondial. Astfel, depistarea şi combaterea devine mult mai complexă, din moment ce programele malware regionale sunt depistate mai rar de către sistemele globale de detecţie, şi necesită nişte sisteme de detecţie mai regionalizate.

Recent au avut loc însemnate atacuri online comise de grupuri auto-intitulate anonime, care iau în obiectiv, în prezent, infrastructurile de încredere, cum ar fi companiile de securitate online şi autorităţile de certificare.

În acelaşi timp, multe ţări şi-au dezvoltat şi consolidat aptitudinile informatice ale instituţiilor militare şi ale securităţii de stat, iar numărul atacurilor informatice sponsorizate de diferite state este în creştere.

Scopul studiului creat de Consiliul Europei este să funcţioneze drept document de politici pentru solicitările de cooperare pentru combaterea criminalităţii informatice în general, să ofere îndrumare foarte practică privind respectarea legislaţiei penale pentru organele de aplicare a legii şi furnizorii de servicii de toate dimensiunile şi din toate ţările, pentru a se ajunge la ceva foarte practic şi util, şi pentru a se confirma că abordarea minimă comună pentru organele de aplicare a legii şi furnizorii de servicii din toate ţările este importantă.

Obiectivul primar a fost să se cartografieze cele mai bune practici în sensul respectării legislaţiei penale de la nivel mondial, iar această definiţie a celor mai bune practici a vizat instituirea unui nivel de uniformitate în ceea ce priveşte interacţiunea zilnică şi cooperarea pe termen lung dintre respectivul sector şi organele de aplicare a legii.

Printre obiectivele secundare se includ:

- Formare – Elaborarea şi coordonarea de programe de formare pe tendinţele criminalităţii informatice şi mijloacele eficiente de a o combate
- Partajare de cunoştinţe – Susţinerea şi coordonarea de conferinţe pentru partajarea de cunoştinţe colective legate de combaterea criminalităţii informatice
- Instrumentele de sprijin – crearea şi/ sau susţinerea de instrumente pentru a sprijini organele de aplicare a legii în special în situaţiile în care strângerea şi păstrarea datelor în cursul unei descinderi sau de pe calculatoarele confiscate, managementul investigaţiilor, transmiterea de probe necesare organelor de aplicare a legii sunt complexe

Dacă organele de aplicare a legii au răspunderea prevenirii şi investigaţiei infracţionalităţii şi sunt la curent cu tendinţele criminalităţii informatice, sectorul ICT este victima infracţionalităţii şi la curent cu câteva tendinţe ale criminalităţii informatice şi deţine date referitoare la clienţii care sunt făptuitorii sau victimele actelor infracţionale. Toate acestea necesită legislaţie eficientă care să pună în balanţă instrumentele de anchetă şi drepturile fundamentale la intimitatea comunicaţiilor şi dreptul persoanelor de a fi protejate împotriva activităţilor infracţionale.

Obiectivele esenţiale ale liniilor directoare pentru organele de aplicare a legii şi sectorul ICT au fost:

- Bazate pe legislaţiile naţionale actuale
- Să asigure echilibrul şi echitatea
- Să consolideze drepturile omului şi rolul procesului democratic
- Să aibă o aplicare generală
- Să încurajeze neutralitatea legislativă

- Să nu fie un înlocuitor al sistemelor sau al procedurilor judiciare

Provocarea Solicitărilor de Date

Succesul ambelor anchete, naţionale şi internaţionale, de criminalitate informatică depinde foarte mult de disponibilitatea anumitor date. Accesul la astfel de date poate permite autorităţilor de aplicare a legii să îi identifice pe infractori sau să închidă serverele care găzduiesc conţinut ilegal. În majoritatea situaţiilor, datele relevante nu se află în posesia organizaţiilor statului, ci sunt generate şi stocate de actorii din cadrul sectorului. Prin urmare, solicitările privind datele deţinute primite din partea organelor de aplicare a legii reprezintă un domeniu important de cooperare.

De obicei, există două motive principale pentru care organele de aplicare a legii înaintează solicitări de date sectorului ICT , inclusiv pentru strângerea de informaţii operative penale/ naţionale, dar şi pentru aspectele judiciare ale unei cercetări penale, printre care se includ:

- Identificarea făptuitorilor
- Strângerea de probe
- Exonerarea Părţilor Terţe Nevinovate

Printre tipurile de date implicate se includ date privind abonaţii, date de trafic, date de conţinut, date de facturare şi date privind organizaţiile.

Printre aspectele privind accesul la date se includ păstrarea datelor, menţinerea cu celeritate, dezvăluirea cu celeritate, producerea datelor, percheziţie şi confiscare, interceptarea legală, impactul asupra dreptului la viaţă intimă şi la protecţia datelor cu caracter personal

Paşi în sensul cooperării

Nici o organizaţie care lucrează individual nu poate spera să

reducă actele de criminalitate de pe internet. Organizaţiile naţionale şi internaţionale trebuie să colaboreze pentru elaborarea de soluţii cuprinzătoare care să conducă la un progres în scopul protejării utilizatorilor de internet de criminalitate.

Există un set de măsuri care se pot lua pentru a realiza acest scop, prin stimularea culturii de cooperare, iar susţinerea activă a unei culturi de parteneriate public privat este esenţială pentru a avea succes.

Scopul acestor paşi este să sprijine organizaţiile care doresc să lase o amprentă, dar care tot trebuie să se organizeze astfel încât să partajeze abundenţa de aptitudini şi cunoştinţe pe care le-au dobândit pentru profitul nostru al tuturor.

Pasul 1 – Diseminarea Liniilor Directoare ale Consiliului Europei în scopul cooperării dintre organele de aplicare a legii şi sectorul de internet

Consiliul Europei a publicat nişte linii directoare cuprinzătoare în 2008 (Anexa I – Linii directoare) prin care a încurajat furnizorii de servicii de internet şi organele de aplicare a legii să colaboreze mai îndeaproape. Există dovezi clare că documentul de orientare a fost tradus în mai multe limbi şi că a fost pus în circulaţie la scală largă, dar încă mai trebuie întreprinse măsuri pentru ca multe aspecte să fie convertite la contextul naţional astfel încât să aibă finalitate practică. Se speră ca următorii paşi să poată sprijini acest proces de punere în practică a liniilor directoare.

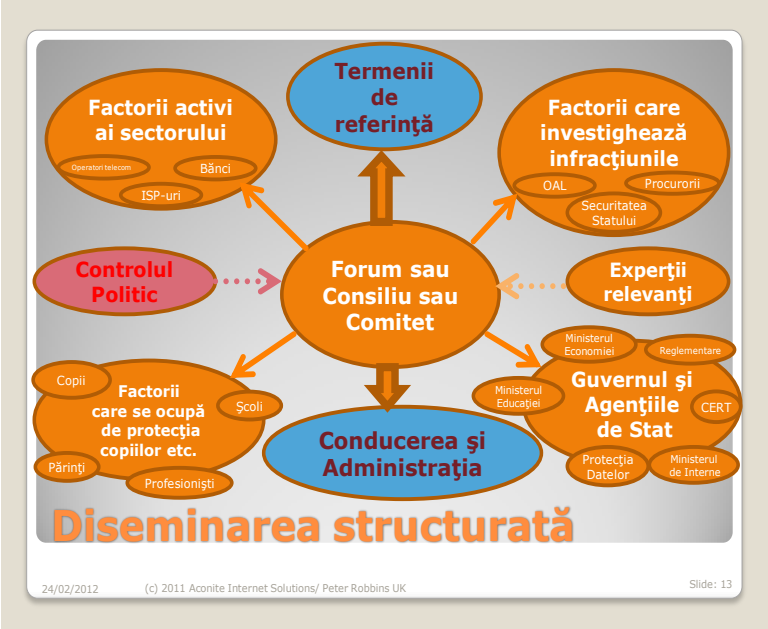
Pasul 2 – Exerciţiile naţionale de re-examinare

Ar fi înţelept dacă personalul cu experienţă ar pune în practică o activitate de trecere în revistă pentru a vedea dacă s-ar putea consolida orice grup de cooperare oficial sau neoficial existent.

A devenit evident că existau deja aplicate câteva proiecte naţionale de siguranţă pe internet în România, Ungaria şi Bulgaria, şi, deci, există oportunitatea reală să se ia contactul cu coordonatorii acestor proiecte pentru a se vedea dacă participanţii ar fi pregătiţi să accepte noi participanţi prin, eventual, modificarea structurii. Posibilitatea de fuzionare a câtorva dintre grupuri sau crearea de sub-comitete pe baza unui comitet central existent ar putea conduce la economii de scală, la o eficienţă şi eficacitate sporite, precum şi la partajarea responsabilităţii, în sensul dezbaterii formatului cel mai eficient din punct de vedere al costului pentru toate părţile.

Pasul 3 – Partajarea structurată prin intermediul creării unui forum naţional

Se recomandă cu căldură crearea unui forum naţional care să reunească laolaltă actori esenţiali din cadrul sectorului şi al structurii guvernamentale, care să îşi partajeze cunoştinţele şi să elaboreze politici adecvate pentru fiecare ţară, bazate pe încredere, deschidere şi transparenţă.



Pasul 4 – Identificarea rolurilor de coordonare

Personalului cu experienţă de la nivelul organismelor esenţiale îi revine sarcina de a îşi dedica câteva dintre resursele lor valoroase pentru instituirea unui forum în care participanţii să se reunească. Viziunea acestora, angajamentul lor pentru un scop comun este esenţial dacă se doreşte înfiinţarea unui forum cu o durată îndelungată de activitate.

Pasul 5 – Crearea termenilor de referinţă

În primul rând, grupul/ comitetul/ forumul ar trebui să discute şi să convină asupra câtorva termeni de referinţă care ar trebui interpretaţi într-un stadiu preliminar, ca o etapă însemnată de consolidare a încrederii dintre părţi.

Există foarte multe exemple excelente de termeni de referinţă online, dar pentru a sprijini reflecţia, iată câteva exemple:

- (se inserează denumirea organismului) aduce laolaltă sectorul de stat, sectorul privat, organele de aplicare a legii, universităţile şi fundaţiile de caritate pentru a lucra în parteneriat în scopul de a îi ajuta pe consumatorii de internet să navigheze în siguranţă în mediul online.
- Pentru promovarea, menţinerea şi consolidarea unei relaţii de lucru eficace şi proporţională între sectorul privat, sectorul de stat şi organizaţiile de aplicare a legii pentru a combate criminalitatea şi pentru a stimula încrederea în ceea ce priveşte utilizarea internetului.
- Promovarea unui mediu deschis şi de cooperare.
- Pentru a institui relaţii de lucru cu celelalte forumuri de combatere a fraudelor din străinătate.
- Pentru a forma alianţe strategice cu organismele de consumatori şi a intermedia relaţia cu furnizorii de servicii.
- Pentru a identifica riscurile de fraudare
- Pentru a identifica şi defini metodele de fraudare
- Pentru a genera documentaţia adecvată şi pentru a spori nivelul de conştientizare cu privire la instrumentele şi metodele tangibile în vederea sprijinirii sectorului privat să gestioneze mai eficient fraudele
- Pentru a examina şi evalua abordările curente de la nivelurile naţional şi internaţional, pentru a soluţiona problema utilizării ilegale şi nocive a internetului.
- Pentru a identifica problemele juridice, tehnice şi structurale care apar şi pentru a face recomandări concrete în sensul soluţionării acestora pe termen scurt, mediu şi lung, aşa cum se impune.
- Pentru a emite recomandări, în legătură cu aceste aspecte care trebuie soluţionate într-un context internaţional, care să stea la baza politicilor aplicabile în această privinţă.
- Pentru a contribui la monitorizarea şi implementarea deciziilor UE şi ONU referitoare la siguranţa pe internet

- Pentru a oferi consiliere cu privire la priorităţile de cercetare în acest domeniu
- Pentru a oferi consiliere cu privire la creşterea nivelului de conştientizare legată de utilizarea ilegală şi nocivă a internetului
- Pentru a oferi consiliere cu privire la elaborarea mecanismelor de implicare a actorilor esenţiali
- Pentru a examina şi evalua abordările actuale de la nivelurile naţional şi internaţional legate de soluţionarea problemei utilizării ilegale şi nocive a internetului

Pasul 6 – Recunoaşterea diferitelor roluri şi atribuţii

Încrederea nu apare dintr-odată. Apare în timp, şi este necesară înţelegerea, însă, cu toate astea, personalităţilor implicate le revine sarcina să respecte contribuţia tuturor părţilor în sensul îndeplinirii scopului global. Uneori, vor fi necesare compromisuri şi bunăvoinţă de partea ambelor părţi pentru a permite apariţia progreselor. Din moment ce parteneriatele implică membrii ai diferitelor discipline, cea mai mare provocare o constituie crearea egalităţii şi a relaţiilor de lucru satisfăcătoare.

Pasul 7 - Eforturile pentru a ajunge la o înţelegere mai bună a rolurilor şi a atribuţiilor tuturor părţilor implicate

Un aspect esenţial al progresului relaţiei îl constituie recunoaşterea rolului fiecărei părţi şi a constrângerilor de funcţionare cu care se confruntă. Uneori, aderarea strictă la anumite responsabilităţi poate da impresia că stă în calea progresului, de aceea este important să se accepte situaţia şi să existe concentrare pe părţile comune, acolo unde nu există riscul nerespectării limitelor.

Pasul 8 – Acordul asupra unui calendar al reuniunilor

Este recomandabil ca grupul să convină asupra periodicităţii reuniunilor şi ca membrii să se angajeze în nume personal să îşi facă timp să participe în loc să delege mult prea frecvent reprezentanţi pentru a participa în locul lor.

Pasul 9 – Identificarea şi clarificarea

Identificarea şi clarificarea necesităţilor fiecărui sector. Acesta este un exerciţiu excelent pentru ca participanţii să se concentreze încă de la începutul procesului. Sesiunea moderată pentru a cartografia împreună aspectele sectoarelor pe care le au în vedere că vor conta poate conduce la identificarea problemelor comune asupra cărora să se lucreze în continuare.

Pasul 10 - Împărtăşira de cunoştinţe şi aptitudini legate de tendinţele şi experienţele cu criminalitatea

Ambele părţi deţin date cuprinzătoare referitoare la tendinţe care, dacă sunt împărtăşite ar putea conduce la prevenirea infracţionalităţii prin introducerea de noi procese care să îi pună stavilă.

În plus, cu siguranţă infractorii vor încerca să exploateze decalajele pe măsură ce progresează tehnologiile, aşa că, cu cât mai curând se identifică vulnerabilităţile, cu atât mai curând pot fi soluţionate.

Pasul 11 - Solicitarea sprijinului politic

Se sugerează ca foarte de timpuriu în cursul procesului să se invite liderii politici să fie parte integrantă a parteneriatului. Prezenţa acestora atrage după sine experienţa considerabilă şi face dovada angajamentului acestora în sensul prevenirii şi soluţionării criminalităţii. Contribuţia acestora, împreună cu resursele aflate la dispoziţia lor, face ca ei să preia firesc

preşedinţia grupului. Dacă un politician nu poate să participe, atunci funcţionarii guvernului reprezintă o alternativă excelentă, deşi nu se estimează că ei vor prezida reuniunile decât dacă aceasta este dorinţa Comitetului/ Forumului/ Membrilor.

Pasul 12 - Elaborarea de politici convenite reciproc

După ce grupul îşi va fi consolidat şi încrederea şi nivelul de înţelegere, îi va veni firesc la îndemână să elaboreze politici convenite reciproc, care ar putea fi proiectate şi publicate. Nu ar trebui subestimată importanţa de a demonstra publicului larg că grupul este hotărât să conlucreze pentru a combate criminalitatea informatică.

Pasul 13 – Formarea în comun

Organizarea de formare în comun cu privire la noile tehnologii, precum şi la noile instrumente juridice şi chestiunile relevante în curs de dezvoltare

Un astfel de forum oferă o ocazie extraordinară pentru membri să-şi împărtăşească unii altora şi să afle despre noile progrese din propria lor sferă de operaţiuni, pe măsură ce apar noi tehnologii sau se adoptă noi directive sau legi, astfel încât forumul să fie pus la curent în legătură cu schimbările apărute. Alternativ, forumul ar putea fi utilizat ca o platformă robustă sau o platformă pentru consultări oficiale şi neoficiale în momentul în care se au în vedere noi legi sau noi tehnologii.

În contextul prezentului proiect, una dintre discuţiile timpurii s-ar putea raporta la folosirea de formulare standardizate. Înainte de lansarea formularelor, ar trebui să existe un proces de asimilare al acestora de către organizaţii, pentru a fi cunoscute, pentru ca organizaţiile să poată modifica sau îmbunătăţi şabloanele şi pentru a le fi oferit timp organizaţiilor să le introducă în strategia în curs.

Pasul 14 – Punctul Unic de Contact (SPOC)

Punctul Unic de Contact este un concept a cărui popularitate este în creştere din cauza numărului sporit al solicitărilor şi a lipsei canalelor care să le permită solicitărilor să circule între părţile implicate. Majoritatea furnizorilor mari de servicii electronice naţionali şi internaţionali şi-au centralizat procedurile de respectare a legislaţiei penale pentru a gestiona solicitările primite şi soluţionate, însă nu acelaşi lucru este valabil şi pentru instituţiile publice care par să continue să facă solicitările într-un mod lipsit de coordonare.

Crearea unui Punct/ Birou/ Specialist Unic de Contact, prin intermediul căruia să fie prelucrate toate solicitările nu este o idee nouă, însă crearea acestui grup de parteneriat i-ar putea permite sectorului privat să explice de ce ar dori să existe un SPoC. Această situaţie ar putea conduce la schimbări structurale pentru anumite activităţi ale organelor de aplicare a legii, însă, dacă nu se analizează avantajele prin preluarea bunelor practici existente în alte părţi ale lumii, atunci va continua să existe o lipsă de eficienţă în cazul schimburilor de date, de care vor beneficia infractorii.

Pasul 15 – Ghidurile sectorului privat de respectare a legislaţiei penale pentru organele de aplicare a legii

Mulţi mari furnizori naţionali şi multinaţionali de servicii publică linii directoare pentru scopurile organelor de aplicare a legii, în care explică gama de servicii pe care le furnizează şi cum trebuie făcute cererile pentru a avea acces la datele acestora. Personalul organelor de aplicare a legii are acces la aceste ghiduri şi se asigură că sunt puse la dispoziţia tuturor celor care vor să le studieze dintre membrii lor. SPoC ar fi locul ideal în care să fie gestionate aceste ghiduri.

Pasul 16 - Ar trebui dezvoltate sistemele de înştiinţare

şi de blocare (NTD) o dată cu investigaţiile penale

La Anexa V – Formular de Înștiințare si Închidere a fost inclus un şablon însă este sarcina grupului de parteneri să aibă în vedere modalităţile prin care poate fi comunicată o astfel de înştiinţare, de către cine şi care sunt consecinţele juridice în cazul în care se ignoră înştiinţarea.

Pasul 17 – Soluţionarea problemelor

În sfârşit, grupul de parteneri se va putea bizui pe talentele membrilor pentru a soluţiona majoritatea problemelor. S-ar putea să dureze soluţionarea problemelor, însă va fi un timp care nu va fi irosit în van. Cele trei aspecte care ar putea fi avute în vedere drept puncte principale ale ordinii de zi ar fi crearea unui Punct Unic de Contact în cadrul Organelor de Aplicare a Legii, adoptarea sau adaptarea formularelor standardizate şi elaborarea unei politici pentru emiterea şi transmiterea Înştiinţărilor legate de Blocarea Conţinutului de Pornografie Infantilă.

Implementarea Studiului de Caz – Experienţele maghiare în urma activităţilor din cadrul proiectului

Reprezentanţii din Ungaria au redactat deja o recomandare cu privire la modul în care trebuie puse în practică liniile directoare de mai sus, care a fost acceptată de Procurorul General.

Pe scurt, recomandarea se referă la următoarele.

1. Consolidarea cooperării dintre sectoarele public şi privat

Se poate face prin

- acceptarea celor două acorduri alăturate privind

cooperarea cu furnizorii de servicii

- elaborarea de formulare standardizate de cerere pentru furnizori. Formularele standardizate elaborate în cursul proiectului vor reprezenta un punct bun de plecare în această privinţă. Chiar dacă cea mai eficientă soluţie ar fi să existe un formular generalizat pentru toţi furnizorii, poate să nu fie fezabil pe termen scurt din cauza sistemelor diferite care se utilizează.
- pregătirea frecventă a personalului din organele de aplicare a legii cu privire la progresele tehnologice, cu ajutorul furnizorilor
- discuţiile frecvente ale problemelor cu care ne confruntăm în cursul cooperării
- comunicat de presă cu privire la acordurile de cooperare (deoarece are în general un efect de prevenire a criminalităţii)
- implementarea de metode automatizate de a răspunde la solicitări (de către furnizorii de telecomunicaţii cu care suntem în negocieri permanent)

2. Îmbunătăţirea schimbului de informaţii la nivelul autorităţilor de aplicare a legii

- Autorităţile maghiare au o gamă largă de cunoştinţe cu privire la progresele tehnologice. Ca în multe alte ţări, unele cadre ale organelor de aplicare a legii şi unii procurori deţin doar cunoştinţe de bază – ştiu cum să înainteze cererile relevante, însă nu au fost pregătiţi de furnizorii de servicii cu privire la modul în care le funcţionează acestora sistemele şi nici cu privire la tipurile de informaţii pe care le pot solicita în mod legal. Unii dintre ei au cunoştinţele generale adecvate pentru a continua anchetele complexe din mediul IT, însă au nevoie de actualizarea permanentă a aptitudinilor şi cunoştinţelor proprii pentru a înţelege noile servicii şi hardware. O minoritate deţine cunoştinţe tehnice excelente şi pe aceasta te poţi bizui în cazul dosarelor complexe de

criminalitate informatică. La fel şi în cazul echipamentului de analiză a sistemelor informatice, care este, de asemenea, variabil, deoarece majoritatea autorităţilor nu deţin echipamentul adecvat sau cunoştinţele corespunzătoare pentru a-l putea folosi cum trebuie.

- E imposibil să pregăteşti pe toată lumea să fie cea mai bună în problemele de tehnologie şi să faci pregătirea mai multor sute de procurori cu ajutorul furnizorilor. Ungaria trebuie să accepte provocarea referitoare la scala pregătirii necesare, însă, cu toate acestea, într-o lume ideală, toate organele de aplicare a legii şi procurorii ar trebui să beneficieze, cel puţin de pregătirea de bază pe problemele tehnice, altfel nu îşi pot îndeplini eficient rolul de procurori în materia criminalităţii informatice, nu pot coordona corespunzător anchetele, nu pot reprezenta corespunzător statul în cadrul procedurilor din instanţă, etc. În prezent, majoritatea dosarelor au dimensiuni tehnologice, deoarece întreaga populaţie foloseşte dispozitive tehnologice, care înregistrează informaţii utile pe care procurorii le pot folosi în cursul anchetelor.
- Din cauza acestei conştientizări, se recomandă instituirea unei structuri pe trei niveluri pentru scopuri de partajare de informaţii la nivelul serviciului de parchet.
- Nivelul superior va fi la Parchetul General şi va răspunde de acordul pentru contractele de cooperare cu furnizorii, va activa drept SPoC în această privinţă, deoarece acceptă feedback-ul de la furnizori, va avea grijă de pregătirea personalului parchetelor prin intermediul sesiunilor personale de formare în direct, dar şi al manualelor şi liniilor directoare scrise. Acest nivel va fi „vârful" structurii, şi va lua chiar şi decizia de achiziţionare a noilor echipamente de criminalistică, dacă este necesar
- Nivelul mijlociu va fi cel al Prim-procurorilor, deoarece aceste organizaţii controlează calitatea activităţii birourilor locale de parchete din fiecare comitat al Ungariei şi la

acest nivel există procurori care sunt pregătiţi să ia decizii generale cu privire la practicile care trebuie respectate, au suficientă experienţă. Prin urmare, aceasta este o bază bună pentru a găsi persoanele care ar putea participa la sesiunile de pregătire în direct şi ar fi pregătite să fie la curent cu tendinţele din tehnologie. Acest nivel ar supraveghea parchetele locale şi le-ar oferi instrucţiuni în materia tehnologiilor. Nivelul mijlociu ar putea activa, de asemenea, ca principale puncte de contact. (Şi ar putea lua legătura cu furnizorii, fără să se mai utilizeze un nivel superior, dacă apare vreo problemă.)

- Cel de-al treilea nivel ar fi cel al parchetelor locale şi al procurorilor locali, care ar fi pregătiţi în cadrul structurii de parchet, de către experţii organizaţiei de la nivelurile mijlociu şi superior, cu ajutorul materialelor scrise.

- Această recomandare nu include până la acest moment un SPoC adevărat, şi nici controlul calităţii. Procurorii şi ofiţerii de poliţie au pregătirea corespunzătoare şi li se poate permite să trimită direct solicitările. Astfel e mult mai rapid decât să se trimită prin intermediul unui SPoC şi tot aşa le-ar primi înapoi. Desigur, efectul secundar nefericit al acestei situaţii este că i se permite unilateral beneficiarului tuturor acestor solicitări să decidă care este nivelul de prioritate al tuturor acestor solicitări şi care este ordinea în care ar trebui completate. Pe măsură ce se maturizează noua generaţie de populaţie, care cunoaşte mai bine internetul, Ungaria va avea mai puţine probleme să obţină informaţii în chestiuni tehnologice. De exemplu, ofiţerii sunt deja familiarizaţi cu solicitările de date de telecomunicaţii şi pot conlucra bine cu controlul general al calităţii efectuat de procurorii care le coordonează activitatea, precum şi de şefii cu mai multă experienţă. În următorii ani, acelaşi lucru se va aplica şi pentru informaţiile privind logarea la internet. Desigur, noile tendinţe vor însemna, în acelaşi timp, noi provocări, dar, pe măsură ce trece timpul, şi procurorii pot fi pregătiţi să

le implementeze. Prin urmare, recomandarea este să se partajeze informaţia şi să existe un model jumătate centralizat, jumătate descentralizat, în loc să existe o centralizare totală a modelului SPoC.

- Pentru acest schimb de informaţii se recomandă, de asemenea, crearea unui forum pe intranetul nostru de către parchet, unde procurorii de la diferitele niveluri să poată discuta problemele, întrebările, răspunsurile, cele mai bune practici între ei, ceea ce ar ajuta să existe o practică similară la nivelul întregii ţări.

3. Progrese internaţionale

- Se recomandă actualizarea paginii de internet a Reţelei Judiciare Europene, pentru a avea detaliile corespunzătoare ale autorităţilor ţărilor străine care vor să transmită o solicitare de AJR pentru a obţine informaţii de la furnizorii maghiari.
- Deoarece în Ungaria există deja reguli pentru contactul direct în UE, solicitări AJR pentru scopuri de clarificare, Ungaria ar putea implementa procedurile de identificare corespunzătoare, cum ar fi utilizarea semnăturii electronice şi la nivelul acestui tip de comunicare. (Semnătura electronică din Ungaria este deja în curs de implementare şi se planifică în curând câte una pentru fiecare procuror)
- Ungaria ar putea crea un forum internaţional pentru împărtăşirea de informaţii privind diferitele aspecte, care ar putea fi similar cu cel menţionat la sfârşitul părţii 2.
- Ungaria ar putea crea un SPoC pentru transmiterea de solicitări pentru marile companii străine, cum ar fi Yahoo, Facebook, Google, etc.

Concluzii

Solicitanţii şi partenerii din cadrul proiectului vor utiliza exhaustiv rezultatele proiectului. Liniile directoare şi formularele standardizate vor fi folosite pentru comunicarea şi schimbul de date cu actorii din sectorul privat şi se vor avea în vedere angajamentele neoficiale transmise în cursul atelierelor pentru definirea politicilor şi a acţiunilor viitoare în domeniul combaterii criminalităţii informatice.

Partenerii la proiect ar trebui să îşi asume experimentarea şi evaluarea periodică a mecanismelor de cooperare create în cadrul prezentului proiect şi să elaboreze noi instrumente în conformitate cu tendinţele infracţionale relevante.

Punctele de contact instituite prin intermediul participării la activităţile din cadrul proiectului ar putea fi utilizate în viitor ori de câte ori schimburile de informaţii şi cele mai bune practici vor fi necesare.

- Lectura liniilor directoare originale
- Re-examinarea Termenilor de Referinţă privind crearea unui parteneriat
- Adoptarea şi consolidarea formularelor pentru respectarea procedurilor penale
- Evaluarea repetată a eficienţei în cooperare

Anexa I – Linii directoare

Liniile directoare ale Consiliului Europei pentru cooperarea dintre organele de aplicare a legii şi furnizorii de servicii de internet împotriva criminalităţii informatice

Introducere

1. Consolidarea unei societăţi informaţionale necesită consolidarea încrederii în tehnologiile informaţiei şi ale comunicaţiilor (ICT's), protecţia datelor cu caracter personal şi a dreptului la viaţă privată, precum şi promovarea unei culturi globale a securităţii informatice într-un context în care societăţile de peste tot din lume depind din ce în ce mai mult de ICT, şi, în consecinţă, sunt din ce în ce mai vulnerabile în faţa criminalităţii informatice;

2. Prima şi cea de-a Doua Reuniune Mondială la Nivel Înalt privind Societatea Informaţională (Geneva 2003, Tunis 2005) – printre altele – angajate să consolideze o societate informaţională incluzivă în care toată lumea să poată crea, accesa, utiliza şi partaja informaţiile şi cunoştinţele, dezvoltându-şi deplin potenţialul şi îmbunătăţindu-şi calitatea vieţii, s-au bazat pe scopurile şi principiile Cartei Organizaţiei Naţiunilor Unite şi au respectat integral şi au susţinut Declaraţia Universală a Drepturilor Omului, care promovează noi forme de parteneriat şi cooperare între guverne, sectorul privat, societatea civilă şi organizaţiile internaţionale;

3. Furnizorii de servicii de internet (ISP) şi organele de aplicare a legii (OAL) joacă un rol esenţial în punerea în practică a acestei viziuni;

4. Legislaţia naţională, în conformitate cu Convenţia privind criminalitatea informatică a Consiliului Europei (în cele ce urmează „Convenţia de la Budapesta") sprijină statele pentru a îşi crea o bază juridică robustă pentru cooperarea dintre public şi privat, competenţele de anchetă, precum şi pentru cooperarea internaţională;

5. Liniile directoare nu intenţionează să se substituie nici unui instrument juridic existent, însă pornesc de la premisa că există instrumentele juridice adecvate care furnizează un sistem bine echilibrat de instrumente de anchetă, precum şi garanţiile conexe şi protecţia drepturilor fundamentale ale omului, cum ar fi libertatea de exprimare, respectul dreptului la viaţă privată, domiciliu şi corespondenţă, precum şi al dreptului la protecţia datelor cu caracter personal. Se recomandă, aşadar, statelor să adopte reglementările ce se impun prin legislaţia lor naţională pentru a pune integral în practică prevederile procedurale ale Convenţiei privind criminalitatea informatică, şi pentru a defini autorităţile de anchetă şi obligaţiile organelor de aplicare a legii, instituind, în acelaşi timp, condiţiile şi garanţiile prevăzute la Articolul 15 al Convenţiei. Acestea vor
   - asigura activitatea eficientă a organelor de aplicare a legii
   - proteja capacitatea furnizorilor de servicii de internet de a îşi oferi serviciile
   - asigura că reglementările naţionale sunt conforme cu standardele globale
   - promova standarde globale în loc de soluţii naţionale izolate
   - ajuta la asigurarea echităţii procedurilor şi a statului de drept, inclusiv a principiilor legalităţii, proporţionalităţii şi necesităţii;

6. În scopurile prezentelor linii directoare, folosim definiţia „furnizorului de servicii” inclusă în Convenţia privind Criminalitatea Informatică la Articolul 1 unde se defineşte „furnizorul de servicii” într-un sens larg, şi înseamnă:

   i orice entitate publică sau privată care oferă utilizatorilor serviciilor sale posibilitatea de a comunica prin intermediul unui sistem informatic, şi

   ii orice altă entitate care prelucrează sau stochează date informatice pentru acest serviciu de comunicaţii sau pentru utilizatorii săi;

7. Pentru a consolida securitatea informatică, diminuarea utilizării serviciilor în scopuri ilegale şi consolidarea încrederii în ICT, este esenţial ca furnizorii de servicii de internet şi organele de aplicare a legii să coopereze unele cu celelalte într-un mod eficient fiind acordată atenţie rolurilor lor respective, costului acestei cooperări şi drepturilor cetăţenilor;

8. Scopul prezentelor linii directoare este să sprijine organele de aplicare a legii şi furnizorii de servicii de internet să îşi organizeze interacţiunile în legătură cu aspectele de criminalitate informatică. Se bazează pe bunele practici existente şi ar trebui să fie aplicabile în orice ţară din lume, în conformitate cu legislaţia naţională şi cu respectul pentru libertatea de exprimare, dreptul la viaţă privată, protecţia datelor cu caracter personal şi alte drepturi fundamentale ale cetăţenilor;

9. Se recomandă ca Statele, organele de aplicare a legii şi furnizorii de servicii de internet să ia următoarele măsuri la nivel naţional:

Linii directoare comune

10. Organele de aplicare a legii şi furnizorii de servicii de internet trebuie să fie încurajaţi să se implice în schimbul de informaţii pentru a îşi consolida capacitatea de a identifica şi combate tipurile de criminalitate informatică existente. Organele de aplicare a legii ar trebui încurajate să informeze furnizorii de servicii cu privire la tendinţele criminalităţii informatice;

11. Organele de aplicare a legii şi furnizorii de servicii de internet trebuie să promoveze mentalitatea de cooperare – mai degrabă decât de confruntare – inclusiv partajarea de bune practici. Se încurajează reuniunile periodice pentru schimbul de experienţă şi soluţionarea problemelor;

12. Organele de aplicare a legii şi furnizorii de servicii trebuie să fie încurajaţi să elaboreze proceduri scrise pentru cooperarea reciprocă. Unde este posibil, ambele părţi ar trebui să fie încurajate să ofere feedback structurat cu privire la funcţionarea acestor proceduri în ceea ce le priveşte;

13. Parteneriatele oficiale dintre organele de aplicare a legii şi furnizorii de servicii trebuie avute în vedere pentru instituirea de relaţii pe termen mai lung cu garanţiile corespunzătoare de ambele părţi că parteneriatul nu va avea impact negativ asupra drepturilor prin lege ale sectorului privat sau nu va interfera cu competenţele prin lege ale organelor de aplicare a legii;

14. Şi organele de aplicare a legii şi furnizorii de servicii de internet trebuie să protejeze drepturile fundamentale ale cetăţenilor, în conformitate cu Organizaţia Naţiunilor Unite şi celelalte standarde aplicabile europene şi internaţionale, cum ar fi Convenţia din 1950 a Consiliului Europei pentru Protecţia Drepturilor Omului şi a Libertăţilor Fundamentale, a Convenţiei Internaţionale din 1966 a Organizaţiei

Naţiunilor Unite privind Drepturile Civile şi Politice, a Convenţiei din 1981 a Consiliului Europei pentru Protecţia Persoanelor cu privire la Prelucrarea Automatizată a Datelor cu Caracter Personal, precum şi legislaţia naţională. Astfel sunt instituite limite rezonabile legate de nivelul posibil de cooperare;

15. Organele de aplicare a legii şi furnizorii de servicii de internet sunt încurajaţi să coopereze unii cu ceilalţi pentru a aplica standardele de protecţie a dreptului la viaţă privată şi a datelor cu caracter personal de la nivelul naţional, dar şi cu privire la fluxurile de date transfrontaliere.

16. Ambele părţi trebuie să acorde atenţie costurilor implicate pentru crearea şi răspunsul la solicitări. Procedurile de elaborat trebuie să aibă în vedere impactul financiar al acestor activităţi, şi trebuie avute în vedere şi aspectele legate de rambursarea cheltuielilor sau compensaţia echitabilă.

Măsuri de luat de către organele de aplicare a legii

17. Cooperarea lărgită şi strategică – Organele de aplicare a legii trebuie încurajate să îi sprijine pe furnizorii de servicii, angajându-se într-o activitate de cooperare lărgită şi strategică cu sectorul respectiv, care să includă desfăşurarea de seminarii periodice de pregătire pe teme tehnice şi juridice, precum şi furnizarea de feedback în urma anchetelor desfăşurate pe baza plângerilor înaintate de furnizorii de servicii, sau pe baza informaţiilor operative strânse pe baza activităţii infracţionale cunoscute şi raportate de furnizorii de servicii;

18. Proceduri pentru solicitări cu valoare juridică obligatorie – Organele de aplicare a legii trebuie încurajate să redacteze proceduri scrise, care să includă măsurile adecvate care trebuie luate, pentru emiterea şi

prelucrarea solicitărilor cu valoare juridică obligatorie, şi să se asigure că solicitările sunt rezolvate în conformitate cu procedurile convenite;

19. Formare – Organele de aplicare a legii trebuie încurajate să ofere pregătire unui set proiectat de membri ai personalului propriu cu privire la modul în care trebuie implementate aceste proceduri, inclusiv modul în care se pot obţine date de la furnizorii de servicii şi cu privire la modul în care trebuie să prelucreze informaţiile primite, tehnologiile de pe internet şi impactul acestora în general, precum şi cu privire la modul în care trebuie să respecte echitatea procedurilor şi drepturile fundamentale ale persoanelor;

20. Resurse tehnice – Personalul organelor de aplicare a legii responsabil cu cooperarea cu furnizorii de servicii trebuie să se doteze cu resursele tehnice necesare, inclusiv cu accesul la internet, la o adresă de e-mail a instituţiei, prin care să fie clară denumirea instituţiei afiliate, precum şi alte resurse tehnice care să le permită să primească electronic informaţii într-un mod sigur de la furnizorii de servicii;

21. Personalul desemnat şi punctele de contact – Interacţiunea dintre organele de aplicare a legii şi furnizorii de servicii trebuie să fie limitată la personalul pregătit în acest sens. Organele de aplicare a legii trebuie încurajate să desemneze puncte de contact pentru cooperarea cu furnizorii de servicii;

22. Autoritatea pentru solicitări – Organele de aplicare a legii trebuie încurajate să definească clar în procedurile lor scrise care este tipul de personal al organelor de aplicare a legii care poate autoriza şi ce tip de măsuri poate autoriza şi emite solicitări către furnizorii de servicii de internet, şi cum pot fi validate/ autentificate aceste solicitări de către furnizorii de servicii de internet;

23. Organele de aplicare a legii trebuie încurajate să pună la dispoziţia furnizorilor de servicii de internet procedurile utilizate şi, dacă este posibil, care sunt persoanele sau care sunt funcţiile nominalizate care răspund de cooperarea cu furnizorii de servicii de internet;

24. Verificarea sursei solicitării – Sursa solicitării unui organ de aplicare a legii ar trebui să poată fi verificată de furnizorii de servicii:

25. Solicitări – Solicitările din partea organelor de aplicare a legii către furnizorii de servicii trebuie făcute în scris (sau în orice alt mod electronic acceptabil conform legii) şi să poată fi identificat circuitul acestora. În cazurile extrem de urgente, atunci când sunt acceptabile solicitările orale, acestea trebuie imediat urmate de documentaţie scrisă (sau în orice alt mod electronic acceptabil conform legii);

26. Formatul standard de solicitare – La nivel naţional, şi, dacă este posibil, la nivel internaţional, organele de aplicare a legii trebuie încurajate să standardizeze şi să îşi structureze formatul utilizat pentru transmiterea de solicitări şi pentru răspunsurile la solicitări. La modul minim, solicitările trebuie să includă următoarele informaţii:

    - Numărul de înregistrare
    - Referinţa la baza juridică
    - Datele specifice solicitate
    - Informaţia pentru a verifica sursa solicitării;

27. Specificitatea şi precizia solicitărilor – Organele de aplicare a legii trebuie încurajate să se asigure că solicitările transmise sunt concrete, complete şi clare şi că oferă un nivel suficient de detaliu pentru a le permite furnizorilor de servicii să identifice datele relevante. Trebuie încurajate să se asigure că sunt transmise solicitările către furnizorul de servicii care deţine

înregistrările. Trebuie evitate solicitările pentru date multiple şi nespecificate;

28. Organele de aplicare a legii trebuie încurajate să pună la dispoziţie cât mai multe informaţii despre investigaţie cu putinţă, fără a pune în pericol ancheta sau orice drepturi fundamentale, pentru a le permite furnizorilor de servicii să identifice datele relevante;

29. Organele de aplicare a legii trebuie încurajate să ofere explicaţii şi asistenţă furnizorilor de servicii cu privire la tehnicile de anchetă fără legătură cu dosarul pentru ca aceştia să înţeleagă mai bine cum cooperarea lor poate conduce la anchete mai eficiente pentru combaterea criminalităţii şi o mai bună protecţie a cetăţenilor;

30. Prioritizare – Organele de aplicare a legii trebuie încurajate să îşi prioritizeze solicitările, în special cele referitoare la volume mari de date, pentru a le permite furnizorilor de servicii să le soluţioneze mai întâi pe cele mai importante. Prioritizarea se face cel mai bine într-un mod consecvent la nivelul organelor naţionale de aplicare a legii, şi, dacă este posibil, la nivel internaţional;

31. Adecvarea cererilor – Organele de aplicare a legii trebuie încurajate să aibă în vedere costul solicitării pentru furnizorii de servicii şi să le ofere furnizorilor de servicii suficient timp pentru a răspunde. Ar trebui să mai aibă în vedere şi că e posibil ca furnizorii de servicii să trebuiască să răspundă la solicitări şi din partea altor organe de aplicare a legii şi trebuie încurajate să monitorizeze cu atenţie volumele înaintate;

32. Confidenţialitatea datelor – Organele de aplicare a legii trebuie să asigure confidenţialitatea datelor primite;

33. Evitarea cheltuielilor nejustificate şi blocarea activităţii comerciale – Organele de aplicare a legii trebuie încurajate să evite cheltuielile nejustificate şi blocarea activităţii comerciale a furnizorilor de servicii şi a altor tipuri de societăţi comerciale;

34. Organele de aplicare a legii trebuie încurajate să limiteze utilizarea serviciului de puncte de contact de urgenţă doar la cazurile urgente, pentru a asigura că nu se face abuz de acest serviciu;

35. Organele de aplicare a legii trebuie încurajate să se asigure că dispoziţiile de păstrare şi alte măsuri provizorii sunt urmate la timp de dispoziţii de dezvăluire sau că este informat furnizorul de servicii de internet la timp că datele păstrate nu mai sunt necesare;

36. Solicitări internaţionale – În cazul solicitărilor adresate furnizorilor străini de servicii de internet, organele naţionale de aplicare a legii trebuie încurajate să nu direcţioneze solicitările direct către furnizorii străini de servicii de internet ci să utilizeze procedurile descrise în tratatele internaţionale, cum ar fi Convenţia privind Criminalitatea Informatică şi reţeaua de puncte de contact a organelor de aplicare a legii care funcţionează non-stop pentru măsuri urgente, inclusiv dispoziţiile/ solicitările de păstrare;

37. Solicitări de asistenţă judiciară reciprocă internaţională – Organele de aplicare a legii şi autorităţile justiţiei penale trebuie încurajate să ia măsurile necesare pentru a se asigura că solicitările pentru măsuri provizorii sunt urmate de proceduri internaţionale pentru asistenţă judiciară reciprocă sau că furnizorul de servicii de internet este informat la timp că datele păstrate nu mai sunt necesare;

38. Coordonarea dintre organele de aplicare a legii – organele de aplicare a legii trebuie încurajate să îşi coordoneze cooperarea cu furnizorii de servicii de internet şi să partajeze bune practici unii cu ceilalţi la nivelurile naţional şi internaţional. La nivelul internaţional trebuie să utilizeze organismele reprezentative internaţionale relevante în acest scop;

39. Programele de respectare a procedurilor penale – Organele de aplicare a legii trebuie încurajate interacţiunile subliniate mai sus cu furnizorii de servicii sub forma unui program cuprinzător de respectare a procedurilor şi să ofere o descriere a unui astfel de program pentru furnizorii de servicii, inclusiv:

    - Informaţiile necesare pentru a contacta personalul organelor de aplicare a legii desemnat să se ocupe de respectarea procedurilor penale, precum şi orele la care sunt disponibile aceste persoane
    - Informaţiile necesare pentru ca furnizorul de servicii să poată furniza documente către personalul însărcinat cu respectarea procedurilor
    - Alte elemente specifice pentru personalul desemnat din partea organelor de aplicare a legii cu respectarea procedurilor penale (cum ar fi măsura în care un organ de aplicare a legii cooperează cu mai multe ţări, documentele de tradus într-o anumită limbă etc.);

40. Auditul sistemului de respectare a procedurilor – Organele de aplicare a legii trebuie încurajate să monitorizeze şi să auditeze sistemul de prelucrare al solicitărilor în scopuri statistice, pentru identificarea punctelor forte şi a vulnerabilităţilor şi pentru a le publica rezultatele, dacă se impune;

Măsuri de luat de către furnizorii de servicii

41. Cu respectarea drepturilor şi libertăţilor aplicabile, cum ar fi libertatea de exprimare, dreptul la viaţă privată şi alte legi naţionale sau internaţionale, precum şi a acordurilor cu utilizatorii, furnizorii de servicii trebuie încurajaţi să coopereze cu organele de aplicare a legii, pentru a contribui la diminuarea măsurii în care se folosesc serviciile pentru activitatea infracţională, definită prin lege;

42. Furnizorul care este conştient de activitatea infracţională care afectează serviciul de internet oferit trebuie

încurajat să o raporteze organelor de aplicare a legii, ceea ce nu trebuie să îi oblige pe furnizorii de internet să caute activ fapte sau circumstanţe care indică activităţile ilegale;

43. Trebuie încurajaţi să sprijine serviciile şi operaţiunile organelor de aplicare a legii cu educare, formare şi alte activităţi.

44. Trebuie încurajaţi să facă toate eforturile rezonabile să sprijine organele de aplicare a legii pentru a executa solicitarea;

45. Trebuie încurajaţi să redacteze proceduri scrise, care să includă măsurile adecvate care trebuie luate pentru prelucrarea solicitărilor şi să se asigure că solicitările sunt monitorizate conform procedurilor convenite;

46. Trebuie încurajaţi să se asigure că personalul propriu care are sarcina de a implementa aceste proceduri este suficient de bine pregătit;

47. Trebuie încurajaţi să desemneze personalul pregătit drept puncte de contact pentru cooperarea cu organele de aplicare a legii;

48. Trebuie încurajaţi să stabilească mijloacele prin care organele de aplicare a legii pot ajunge la personalul lor responsabil cu respectarea procedurilor penale în afara programului normal de activitate în cazul situaţiilor urgente. Furnizorii de servicii trebuie încurajaţi să le ofere organelor de aplicare a legii informaţiile relevante pentru asistenţa de urgenţă;

49. Trebuie încurajaţi să ofere puncte de contact sau persoane responsabile cu cooperarea cu organele de aplicare a legii, cu resursele necesare care să le permită să respecte solicitările venite din partea organelor de aplicare a legii;

50. Trebuie încurajaţi să îşi organizeze cooperarea cu organele de aplicare a legii sub forma unor programe

cuprinzătoare de respectare a procedurilor penale şi să ofere o descriere a acestor programe către organele de aplicare a legii, incluzând:

- Informaţiile necesare pentru contactarea personalului desemnat din partea furnizorilor, responsabil pentru respectarea procedurilor penale, precum şi orele între care acest personal le stă la dispoziţie
- Informaţiile necesare pentru ca organele de aplicare a legii să poată furniza documente către personalul responsabil cu respectarea procedurilor penale
- Alte elemente specifice pentru personalul responsabil cu respectarea procedurilor penale (cum ar fi măsura în care un furnizor de servicii operează în mai multe ţări, documentele care trebuie traduse într-o anumită limbă etc.);
- Pentru a le permite organelor de aplicare a legii să facă solicitările concrete şi adecvate, furnizorii de servicii trebuie încurajaţi să ofere informaţii cu privire la tipurile de servicii oferite utilizatorilor, inclusiv link-urile web către servicii şi informaţiile suplimentare, precum şi detaliile de contact pentru informaţii suplimentare;
- Dacă este posibil, furnizorul de servicii de internet trebuie încurajat să ofere o listă, la cerere, cu tipurile de date care pot fi puse la dispoziţia organelor de aplicare a legii, în cazul fiecărui serviciu, pe baza primirii unei solicitări valabile de informare din partea organelor de aplicare a legii prin care se acceptă că nu toate aceste date vor fi disponibile pentru toate anchetele penale;

51. Verificarea surselor solicitărilor – Furnizorii de servicii trebuie încurajaţi să ia măsurile ce se impun pentru verificarea autenticităţii solicitărilor primite din partea organelor de aplicare a legii în măsura posibilului şi în care este necesar, pentru a se asigura că datele clientului nu sunt dezvăluite persoanelor neautorizate;

52. Răspuns – Furnizorii de servicii trebuie încurajaţi să răspundă la solicitările din partea organelor de aplicare a legii în scris (sau în orice alt mod electronic acceptabil conform legii) şi să se asigure că este disponibil un circuit al solicitărilor şi al răspunsurilor, acceptând că acest circuit nu poate include orice date personale;

53. Formularul standardizat de răspuns – Având în vedere formatul solicitărilor transmise de organele de aplicare a legii, furnizorii de servicii trebuie încurajaţi să standardizeze formatul de transmitere a informaţiilor către organele de aplicare a legii;

54. Furnizorii de servicii trebuie încurajaţi să prelucreze solicitările la timp, conform procedurilor scrise pe care le-au definit şi să pună la dispoziţia organelor de aplicare a legii liniile directoare privind întârzierile medii legate de răspunsul la solicitări;

55. Validarea informaţiilor transmise – Furnizorii de servicii trebuie încurajaţi să se asigure că informaţiile transmise organelor de aplicare a legii sunt complete, precise şi protejate;

56. Confidenţialitatea solicitărilor – Furnizorii de servicii trebuie să asigure confidenţialitatea solicitărilor primite;

57. Explicaţia pentru informaţiile care nu sunt furnizate – Furnizorii de servicii trebuie încurajaţi să ofere explicaţii organelor de aplicare a legii care transmit o solicitare, dacă se respinge solicitarea sau dacă nu se pot pune la dispoziţie informaţiile;

58. Auditul sistemului de respectare a procedurilor – Furnizorii de servicii trebuie încurajaţi să monitorizeze şi să auditeze sistemul de prelucrare al solicitărilor în scopuri statistice, pentru identificarea punctelor forte şi a vulnerabilităţilor şi pentru a le publica rezultatele, dacă se impune;

59. Coordonarea dintre furnizorii de servicii – având în vedere reglementările împotriva monopolurilor/ privind concurenţa, furnizorii de servicii trebuie încurajaţi să îşi coordoneze cooperarea cu organele de aplicare a legii şi să partajeze bune practicii la nivelul lor, şi să utilizeze asociaţiile de furnizori de servicii în acest scop.

Anexa II – Atelierul de la Sofia

Participanţi

- Coordonatorul proiectului – D-na Ioana ALBANI (RO) (Procuror)
- D-na Camelia STOINA (RO) (Procuror)
- D-na Florina-Silvia POPA (RO) (Procuror)
- Dl. Viorel BADEA (RO) (Procuror)
- Dl. Catalin BORCOMAN (RO) (Procuror)
- Dl. Daniel FILIP (RO) (Poliţist)
- Dl. Bogdan BADIU (RO) (Poliţist)
- Dl. Bogdan STOICA (RO) (Poliţist)
- Dl. Liviu CHIRITA (RO) Asociaţia Băncilor din România
- Dl. Radu GHIDICEANU (RO) (Asociaţia Naţională a Furnizorilor de Servicii de Internet)
- Dl. Bogdan MANOLEA (RO) (Asociaţia pentru Tehnologie şi Internet)
- Dl. Attila KÖKÉNYESI-BARTOS (HU) (Procuror)
- Dl. Imre SZABÓ (HU) (Procuror)
- Dl. Nedko SACHARIEV (BU) (Manager de proiect)
- D-na Lyubka KABZIMALSKA (BU) (Procuror)
- D-na Detelina YOTOVA (BU) (Procuror)
- Dl. Vladimir ROBOV (BU) (IT- Expert)
- Ceilalţi reprezentanţi din BU care au participat în zile diferite trebuie inseraţi aici
- Dl. Cormac Callanan (IR) (Expert)
- Dl. Peter Robbins (UK) (Expert)
- Dl. Alin TORTOLEA (RO) (Manager de proiect)

	ORDINEA DE ZI Bulgaria
ZIUA 1	**27.09.2011**
09,00 - 09,30	Introducere – prezentare generală a proiectului/ scopului Prezentarea experţilor/ participanţilor/ aşteptărilor
09,30 - 10,30	Prezentarea generală a instrumentelor internaţionale relevante
10,30 -11,00	Experienţa experţilor/ aspecte relevante derivate din activitatea cu instrumente internaţionale
11,00-11,15	Pauză de cafea
11,15 – 12,00	**România** Evaluarea cadrului juridic naţional: Sistemul de probatoriu – admisibilitatea probelor digitale/ interceptărilor comunicaţiilor Cadrul juridic privind criminalitatea informatică
12,15 – 13,00	**Bulgaria** (ca mai sus)
13,00 – 14,00	Prânz
14,00 – 14,45	**Ungaria** (ca mai sus)
14,45 – 15,00	**România** Cadrul juridic privind protecţia datelor cu caracter personal – restricţii
15,00 – 15,15	Pauză de cafea
15,15 – 15,30	**Bulgaria** (ca mai sus)
15,30 – 16,00	**Ungaria** (ca mai sus)
16,00 – 17,00	**Experienţa experţilor/ întrebări şi**

	răspunsuri/ clarificări/ lucrul cu delegaţiile
ZIUA 2	**28.09.2011**
09,00 – 09,30	**România** Cadrul juridic privind cooperarea internaţională/ judiciară şi schimbul de informaţii poliţieneşti prin comparaţie cu schimbul de probe/ identificarea problemelor legate de executarea solicitărilor
09,30 – 10,00	**Bulgaria** (ca mai sus)
10,00 - 10,30	**Ungaria** (ca mai sus)
10,30– 10,45	Pauză de cafea
10,45 - 11,15	Blocarea/ eliminarea pornografiei infantile sau a conţinutului ilegal/ probleme juridice/ tehnice
11,15 – 12,15	Experienţa experţilor/ Întrebări şi răspunsuri/ perspectivele participanţilor
12,15 – 13,00	**România** Cadrul juridic privind activitatea băncilor/ concentrarea pe secretul bancar/ legătura cu OAL/ experienţa/ problemele întâlnite în cazul solicitărilor din partea OAL/ informaţiile furnizate
13,00 - 14,00	Prânz
14,00 - 14,45	**Bulgaria** (ca mai sus)
14,45 - 15,30	**Ungaria** (ca mai sus)
15,30 - 15,45	Pauză de cafea
15,45 – 17,00	**Experienţa experţilor/ întrebări şi răspunsuri/ clarificări/ lucrul cu delegaţiile**

ZIUA 3	**29.09.2011**
09,00 - 10,00	**România** Metodologia de investigaţie în cazul infracţiunilor informatice
10,00 -11,00	**Bulgaria** (ca mai sus)
11,00-11,15	Pauză de cafea
11,15- 12,15	**Ungaria** (ca mai sus)
12,15 – 13,00	**România** Frauda cu carduri de credit/ abuzul legat de banking-ul online
13,00 - 14,00	Prânz
14,00 - 14,45	**Bulgaria** (ca mai sus)
14,45 – 15,30	**Ungaria** (ca mai sus)
15,30-15,45	Pauză de cafea
15,45 – 17,00	**Experienţa experţilor/ întrebări şi răspunsuri/ clarificări/ lucrul cu delegaţiile**
ZIUA 4	**30.09.2011**
09,00- 11,00	Discuţiile participanţilor referitoare la formularele standardizate
11,00-11,15	Pauză de cafea
11,15 - 13,00	Concluzii/ clarificări
13,00 - 16,30	Prânz
	Orice alte chestiuni, discuţii

Anexa III – Atelierul de la Budapesta

Lista participanţilor

Ţara	Numele	Funcţia	Instituţia
România	D-na Ioana ALBANI	Procuror	Parchetul de pe lângă Înalta Curte de Casaţie şi Justiţie din România
România	D-na Camelia STOINA	Procuror	Biroul de Reprezentare şi Cooperare Internaţională – DIICOT
România	D-na Florina POPA	Procuror	DIICOT
România	Dl. Viorel BADEA	Procuror	Direcţia de Investigare a Infracţiunilor de Crimă Organizată şi Terorism - DIICOT
România	Dl. Catalin BORCOMAN	Procuror	DIICOT
România	Dl. Daniel FILIP	Ofiţer de poliţie	Direcţia de Combatere a Criminalităţii Informatice (DFOC) din cadrul Inspectoratului General al Poliţiei Române
România	Dl. Bogdan BADIU	Ofiţer de poliţie	DFOC
România	Dl. Virgil SPIRIDON	Ofiţer de poliţie	IGPR

România	Dl. Liviu CHIRITA	Şeful Comisiei Anti-fraudă	Asociaţia Băncilor din România
România	Dl. Radu GHIDICEANU	Director	Asociaţia Naţională a Furnizorilor de Servicii de Internet din România
România	Dl. Bogdan MANOLEA	Director Executiv	Asociaţia pentru Tehnologie şi Internet
România	Dl. Alin TORTOLEA	Manager de proiect	Parchetul de pe lângă Înalta Curte de Casaţie şi Justiţie din România
Bulgaria	D-na Lyubka KABZIMALSKA	Procuror	Parchetul Oraşului Sofia
Bulgaria	D-na Detelina YOTOVA	Procuror	Parchetul Oraşului Sofia
Bulgaria	Dl. Vladimir ROBOV	Expert IT	Serviciul Naţional de Investigaţii
Marea Britanie	Dl. Peter ROBBINS	Expert	
Irlanda	Dl. Cormac CALLANAN	Expert	
Ungaria	Dl. Tibor NAGY	Procuror, şef de departament	Departamentul de IT, Parchetul General din Ungaria
Ungaria	Dl. Attila KÖKÉNYESI-BARTOS	Procuror	Parchetul local din regiunea Buda
Ungaria	Dl. Imre SZABÓ	Procuror	Institutul Naţional de Criminologie
Ungaria	Dl. János HOMONNAI	Procuror	Departamentul pentru Dosare Speciale, Parchetul General al Ungariei
Ungaria	Dl. Gergely		Microsoft

	DZSINICH		
Ungaria	D-na Tünde IGAZ		Centrul Naţional pentru Cooperare Penală (Biroul Interpol din Ungaria)
Ungaria	Dl. Erik CSUPOR Dl. Gergely SZÉKELY	Director General Directorul Serviciului Juridic	VATERA / Allegroup

Ţara	Numele	Funcţia	Instituţia
Ungaria	Dl. Péter HORVÁTH	Director	PROART – Asociaţia pentru legislaţia privind drepturile de autor
Ungaria	Dl. Ferenc SUBA		CERT-Ungaria
Ungaria	Dl. Péter JAKAB *Dl. György FIALKA* *D-na Katalin SZENES*		Asociaţia Băncilor din Ungaria
Ungaria	Dl. Tibor GAZDAG Dl. Zsolt TÓTH Dl. Zoltán JANKÓ Dl. Zsolt SZABOLCSI Dl. Zoltán MAKÓ		Biroul Naţional de Investigaţii
România	Dl. Sebastian DUMINICA		Vodafone România
	Dl. Christian PERELLA D-na Gabriella CSEH		Facebook

Ungaria	Dl. László Király		Hungarian Telekom
Ungaria	Dl. Béla Tóth		Vodafone Ungaria
Ungaria			Telenor

ORDINEA DE ZI	
ZIUA 1	**15.11.2011**
09,00 - 09,45	**Introducere** **Alocuţiunea de deschidere** – Parchetul General **Prezentarea participanţilor** **Statutul proiectului**
09,45 - 11,15	**Vodafone RO / Vodafone HU / Telecom din Ungaria**
11,15 - 11,45	Pauză de cafea
11,45 – 13,00	**Vatera (Allegroup Ltd.)**
13,00 – 14,00	Prânz
14,00 – 14,45	**Serviciul Parchetul General (Ungaria)**
14,45 – 15,30	**PROART (Asociaţia pentru legislaţia privind drepturile de autor)**
15,30 – 16,00	Pauză de cafea
16,00 – 17,00	Activitatea cu delegaţiile.
ZIUA 2	**16.11.2011**
09,00 – 10,15	**Microsoft**
10,15 - 10,45	Pauză de cafea
10,45 – 12,00	**Facebook**
12,00 - 13,00	**Serviciul Parchetul General (Ungaria)**
13,00 – 14,00	Prânz
14,00 – 15.00	**Centrul Naţional pentru Cooperare Penală (Biroul Maghiar al Interpol)**
15,00 - 15,30	Experienţa delegaţiilor de lucru cu furnizorii de servicii de la nivel naţional/ mondial
15,30 - 16,00	Pauză de cafea
16,00 – 17,00	**Experţii** lucrează cu delegaţiile, împreună cu

	reprezentanţii furnizorilor de telecomunicaţii, servicii de internet şi de comerţ electronic.
ZIUA 3	**17.11.2011**
09,00 - 11,00	**Biroul Naţional de Investigaţii**
11,00 - 11,30	Pauză de cafea
11,30 - 12,15	**Asociaţia Băncilor din Ungaria**
12,15 – 13,00	**CERT – Ungaria**
13,00 – 14,00	Prânz
14,30 - 15,30	Experienţa delegaţiilor care lucrează cu experţii CERT naţionali/ experienţa experţilor/ întrebări şi răspunsuri/ clarificări
15,30 - 16,00	Pauză de cafea
16,00 – 17,00	Experţii lucrează cu delegaţiile împreună cu reprezentanţii asociaţiei băncilor, CERT.
ZIUA 4	**18.11.2011**
09,00 - 11,00	Produsele/ propunerile participanţilor de formulare standardizate
11,00 - 11,30	Pauză de cafea
11,30 - 13,00	Concluzii/ clarificări
13,00 - 16,30	Prânz, discuții

Anexa IV – Masa rotundă de la Bucureşti

Lista participanţilor

Ţara	Numele	Funcţia	Instituţia
România	D-na Gabriela SCUTEA	Adjunctul Procurorului General PÎCCJ	Ministerul Public – Parchetul de pe lângă Înalta Curte de Casaţie şi Justiţie a României (PÎCCJ)
România	Dl. Codruţ OLARU	Procuror Şef al DIICOT	Direcţia de Investigare a Infracţiunilor de Crimă Organizată şi Terorism (DIICOT) din cadrul PÎCCJ
România	D-na Ioana ALBANI	Procuror Şef al Biroului de Criminalitate Informatică din cadrul DIICOT; Coordonatorul proiectului	DIICOT
România	D-na Camelia STOINA	Procuror	Biroul de Reprezentare Internaţională şi Cooperare – DIICOT
România	D-na Florina Popa	Procuror	DIICOT – Vâlcea
România	Dl. Cătălin BORCOMAN	Procuror	DIICOT – Braşov

România	Dl. Viorel BADEA	Procuror	Biroul de Prevenire şi Combatere a Criminalităţii Informatice – DIICOT
România	Dl. Alin TORTOLEA	Manager Public; Manager de proiect	Unitatea de Implementare a Programelor - PÎCCJ
România	Dl. Virgil SPIRIDON	Şeful Biroului de Combatere a Criminalităţii Informatice Office	Biroul de Combatere a Criminalităţii Informatice din cadrul Inspectoratului General al Poliţiei Române (IGPR)
România	Dl. Bogdan BADIU	Ofiţer de poliţie	Biroul de Combatere a Criminalităţii Informatice din cadrul Inspectoratului General al Poliţiei Române (IGPR)
România	Dl. Daniel FILIP	Ofiţer de poliţie	Biroul de Combatere a Criminalităţii Informatice din cadrul Inspectoratului General al Poliţiei Române (IGPR)
România	Dl. Radu GHIDICEANU	Director tehnic executiv	Asociaţia Naţională a Furnizorilor de Servicii de Internet din România

România	Dl. Bogdan MANOLEA	Director executiv	Asociaţia pentru Tehnologie şi Internet
România	Dl. Liviu CHIRIŢĂ	Şeful Comisiei Anti-fraudă	Asociaţia Băncilor din România
România	Dl. Daniel NIŢĂ	Director de Securitate OTP Bank, Membru al Comisiei Anti-fraudă	Asociaţia Băncilor din România
România	Dl. Gheorghe ŞERBAN	Director	Asociaţia Naţională a Furnizorilor de Servicii de Internet din România
România	Dl. Radu Niculiu	Director, Prevenirea Fraudelor şi Securitate	Vodafone România
Ungaria	Dl. Attila KÖKENYESI-BARTOS	Procuror	Parchetul Local al Regiunii Buda
Ungaria	Dl. Imre SZABO	Procuror	Institutul Naţional de Criminologie
Bulgaria	D-na Lyubka KABZIMALSKA	Procuror	Parchetul oraşului Sofia
Bulgaria	D-na Detelina YOTOVA	Procuror	Parchetul oraşului Sofia
Bulgaria	Dl. Vladimir ROBOV	Expert IT	Serviciul Naţional de Investigaţii
Irlanda	Dl. Cormac CALLANAN	Expert în cadrul proiectului	
Marea Britanie	Dl. Peter ROBBINS	Expert în cadrul proiectului	

Republica Cehă	Dl. Tomas DOKULIL	Şeful Diviziei de Combatere a Evaziunii Fiscale şi a Spălării de Bani	Unitatea de Combatere a Corupţiei şi a Criminalităţii Financiare, Poliţia Republicii Cehe
Lituania	Dl. Vidas STASIULIS	Anchetator şef	Biroul Poliţiei Criminale
Republica Slovacă	D-na Danica BORZOVA	Ofiţer de poliţie	Unitatea de Informaţii Operative Financiare, Biroul de Combatere a Criminalităţii Organizate, Poliţia Slovacă
Slovenia	Dl. Primoz KRAGELJ	Anchetator penal	Departamentul de Anchete Informatice, Direcţia de Poliţie Ljubljana
Austria	Dl. Kurt EINZINGER		www.netelligenz.at

ORDINEA DE ZI România	
Ziua 1	**08.12.2011**
09,00 – 09,30	**Înregistrare**
09,30 – 10,30	Alocuţiuni şi prezentările participanţilor D-na Gabriela Scutea – Adjunctul Procurorului General Dl. Codruţ Olaru – Procuror Şef DIICOT
10,30 – 11,30	Prezentarea proiectului de raport
11,30 - 12,00	Pauză de cafea
12,00 – 13,00	Prezentarea proiectelor de formulare
13,00 – 14,30	Prânz
14,30 – 16,00	Discuţie/ Dezbatere privind prezentările
Ziua 2	**09.12.2011**
09,30 – 10,30	Observaţii şi sugestii de amendamente şi recomandări Masă rotundă
10,30 – 11,30	Paşii următori şi Activitatea viitoare
11,30 - 12,00	Pauză de cafea
12,00 – 12,30	Remarci/ discursuri finale
13,30 – 14,00	Prânz
14,00 – 16,30	Reuniunea echipei de proiect

Anexa V – Formular de Înştiinţare şi Închidere

[Aici Denumirea organizaţiei]

Număr de serie:
Codul temeiului: Pornografie infantilă (Material care conţine abuz sexual de minori)

URL: xxxxx.com/download/66595/lolita.3gp.html

Adresa IP: 00.11.22.33
Data/ ora evaluate: 11/00/20?? 05:06:07

Către ----------

Vă rugăm să consideraţi prezenta comunicare drept o înştiinţare oficială [solicitare] de a închide url-urile menţionate anterior despre care am stabilit că prezintă materiale cu potenţial penal conform [se inserează legislaţia relevantă], de exemplu imagine (imagini) cu un copil mai mic de 18 ani.

În conformitate cu Regulamentele Comerţului Electronic (Directiva CE) din 2002, (în mod concret Partea 19), dacă pe serverele dvs. se află orice tip de conţinut care pare ilegal, trebuie să luaţi măsuri de urgenţă pentru a bloca sau a nu permite accesul la aceste informaţii.
[Aici urmează detalii privind mandatul organizaţiei de a emite astfel de înştiinţări]
Am descărcat o copie a acestui material şi am alertat [Organul de Aplicare a Legii dacă este implicată o ONG]. Vă rugăm să luaţi măsurile ce se impun pentru ca respectivul material să fie păstrat şi să nu fie şters sau eliminat până la noi înştiinţări [a se omite dacă înştiinţarea este emisă de un Ofiţer al Organelor de Aplicare a Legii.]
Vă rugăm să confirmaţi primirea prezentei înştiinţări şi măsurile pe care le-aţi luat.
Procedura de contestare a acestei înştiinţări se poate consulta la [inseraţi link-ul cu procedura de apel]
[Denumirea expeditorului]

Anexa VI – Reacţia criminalităţii informatice române – motivaţiile proiectului

CRIMINALITATEA INFORMATICĂ – PROVOCĂRI

- caracterul transfrontalier al infracţiunilor informatice;
- anonimatul şi viteza mare la care pot fi comise infracţiunile;
- lipsa legislaţiei adecvate privind criminalitatea informatică;
- competenţe juridice insuficiente pentru urmărirea penală şi accesul în sistemele informatice;
- competenţele de indisponibilizare nu se aplică bunurilor intangibile cum ar fi datele informatice;
- lipsa armonizării dintre diferitele legislaţii procedurale naţionale referitoare la urmărirea penală a infracţiunilor informatice;
- lipsa personalului specializat şi a echipamentului.

CONVENŢIA DE LA BUDAPESTA 2001 – SCOP

- Armonizarea dreptului material penal naţional (elementele constitutive ale infracţiunilor) precum şi ale prevederilor conexe în domeniul criminalităţii informatice;
- Prevederea, prin intermediul dreptului procedural naţional, a competenţelor necesare pentru investigarea şi urmărirea penală a acestor infracţiuni, precum şi a celorlalte infracţiuni comise cu ajutorul unui sistem informatic;

- Instituirea unui cadru rapid şi eficient pentru cooperarea internaţională.

România a semnat Convenţia în 2001 şi a ratificat-o în 2004.

PROCEDURA PENALĂ NAŢIONALĂ
ANCHETA/ PROCESUL PENAL

ETAPA ANTE-PROCESUALĂ

Scop – strângerea de probe pentru punerea sub acuzare

URMĂRIREA PENALĂ – pe baza probelor strânse în cursul cercetării penale ante-procesuale, activitatea procedurală ulterioară se desfăşoară „cu înştiinţare" cu respectarea anumitor reguli procedurale restrictive (prezenţa avocatului apărării la toate audierile şi în cursul activităţilor procedurale, prezenţa inculpatului în stare de arest, a avocatului acestuia, precum şi 2 martori la percheziţia calculatorului, mandate de arest limitate la 6 luni etc.)

Scop – consolidarea materialului probator pentru întocmirea rechizitoriului

Responsabili – poliţia judiciară sub supravegherea procurorilor (infracţiuni standard), parchetele pentru anumite infracţiuni (omor, viol deosebit de grav etc.)

- **procurorii DIICOT şi ofiţerii de poliţie de la DGCO alocaţi diferitelor dosare (infracţiuni comise de grupările de crimă organizată, infracţiuni împotriva securităţii naţionale, infracţiuni de terorism, criminalitate informatică – „stricto sensu"**

RECHIZITORIUL – setul limitat de fapte pe baza probelor strânse cu privire la acuzaţiile penale concrete

PROCESUL

Judecătorul va lua o decizie cu privire la competenţa pe care o

are (materială /teritorială), la perioada arestului preventiv şi la legalitatea rechizitorului în cursul primei şedinţe de judecată.

Termenele sunt stabilite lunar. Publicitatea procesului se efectuează prin intermediul citaţiilor trimise fiecărui participant (domiciliu sau reşedinţa declarată, sediul arestului)

Probatoriul strâns în cursul urmăririi penale (inclusiv în cursul etapei ante-procesuale) se prezintă/ se susţine în faţa judecătorului.

Nu există nici un sistem special pentru determinarea sentinţelor, cu toate acestea, sunt avute în vedere circumstanţele speciale ale inculpatului (de exemplu, lipsa cazierului penal, recunoaşterea acuzaţiilor, cooperant etc.) sau circumstanţele reale agravante/ atenuante (de exemplu, premeditarea, tentativa etc.)

PREVEDERILE NAŢIONALE REFERITOARE LA COMPETENŢA TERITORIALĂ

Art.3 – Dreptul penal român se aplică infracţiunilor comise pe teritoriul României.

Art.4 – Dreptul penal român se aplică infracţiunilor comise în străinătate de cetăţenii români sau de către un apatrid cu reşedinţa în România.

Art.5 - Dreptul penal român se aplică infracţiunilor comise în străinătate de un cetăţean străin sau de către un apatrid care nu îşi are reşedinţa în România împotriva României sau care au pus în pericol viaţa unui cetăţean român.

Art.6 - Dreptul penal român se aplică de asemenea şi infracţiunilor care nu sunt menţionate la art. 5, dar sunt comise în străinătate de un cetăţean străin sau de un apatrid care nu îşi are reşedinţa în România în condiţiile în care:

a) Infracţiunea este incriminată şi în ţara în care a fost comisă
b) Făptuitorul a fost localizat în România

Atunci când se ia o hotărâre cu privire la instanţa care este competentă să judece, primul criteriu care este avut în vedere este locul în care a fost comisă fapta. Legislaţia română (art.30 C.P.R.) defineşte locul în care a fost comisă fapta drept:

- locul în care a fost comisă activitatea infracţională total sau parţial
- locul în care şi-a produs efectele

RIDICAREA DE OBIECTE Şi ÎNSCRISURI (CODUL DE PROCEDURĂ PENALĂ AL ROMÂNIEI - CPPR)

Art. 96 – Organele judiciare au obligaţia să ridice obiectele şi înscrisurile ce pot servi ca mijloc de probă în procesul penal.

Art.97 - Orice persoană fizică sau persoană juridică, în posesia căreia se află un obiect sau un înscris ce poate servi ca mijloc de probă, este obligată să-l prezinte şi să-l predea, sub luare de dovadă, organului de urmărire penală sau instanţei de judecată, la cererea acestora.

RIDICAREA DE OBIECTE Şi ÎNSCRISURI – LEGEA NR. 508/2004

Art.16 (1) – Când sunt indicii temeinice cu privire la săvârşirea uneia dintre infracţiunile atribuite prin prezenta lege în competenţa Direcţiei de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism, în scopul strângerii de probe sau al identificării făptuitorului, pot fi dispuse următoarele măsuri, în conformitate cu prevederile CPPR sau ale legilor speciale:

- Punerea sub supraveghere a conturilor bancare şi a conturilor asimilate acestora
- Punerea sub supraveghere, interceptarea sau înregistrarea comunicaţiilor (este necesar autorizarea de către instanţă)

- Accesul la sisteme informatice (este necesar autorizarea de către instanţă)

(2) – **Procurorii Direcţiei de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism pot dispune să li se comunice înscrisuri, documente bancare, financiare ori contabile, în original sau în copie, de la orice persoană care le are sau le generează. Persoana menţionată are obligaţia să accepte, în conformitate cu prevederea de la alin. (1).**
(3) – Nerespectarea obligaţiei stipulate la alin. (2) atrage răspunderea penală conform legii.

PREVEDERI SUPLIMENTARE
Cooperarea dintre organele de aplicare a legii şi furnizorii de servicii de internet; linii directoare pentru cooperarea dintre organele de aplicare a legii şi furnizorii de servicii de internet în scopul investigării criminalităţii informatice

Elaborate de grupul de lucru din cadrul Proiectului Consiliului Europei privind Criminalitatea Informatică (octombrie 2007 – martie 2008)

- Adoptate de Conferinţa Globală Octopus privind Criminalitatea Informatică din aprilie 2008
- Susţinute de cercetarea detaliată
- Disponibile în mai multe limbi (www.coe.int/cybercrime)
- La nivelul naţional, ghidul a fost publicat pe www.diicot.ro

LEGISLAŢIA NAŢIONALĂ REFERITOARE LA CRIMINALITATEA INFORMATICĂ
INFRACŢIUNILE PREVĂZUTE PRIN LEGEA NR. 161/2003 – TITLUL III

- Accesul, fără drept, la un sistem informatic – art.42
- Interceptarea, fără drept, a unei transmisii de date informatice sau interceptarea unei emisii electromagnetice – art.43

- Fapta de a modifica, şterge sau deteriora date informatice – art.44
- Transferul neautorizat de date dintr-un sistem neconectat sau dintr-un mijloc de stocare a datelor informatice – art.44
- Fapta de a perturba grav, fără drept, funcţionarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ştergerea sau deteriorarea datelor informatice sau prin restricţionarea accesului la aceste date – art.45
- Fapta de a produce, vinde, de a utiliza dispozitive sau sisteme informatice concepute sau adaptate în scopul săvârşirii uneia dintre infracţiunile prevăzute în Legea nr. 161/2003 – art.46
- fapta de a produce, vinde, de a utiliza o parolă, cod de acces sau alte asemenea date informatice care permit accesul total sau parţial la un sistem informatic în scopul săvârşirii uneia dintre infracţiunile în Legea nr. 161/2003 – art.46
- Falsificarea de date informatice; frauda informatică - art.48; art.49
- Pornografia infantilă – art.51

Art.47; art.50 – Se pedepseşte tentativa

INFRACŢIUNI ASIMILATE
INFRACŢIUNI PREVĂZUTE ÎN CODUL PENAL AL ROMÂNIEI, COMISE PRIN INTERMEDIUL UNUI SISTEM INFORMATIC

Ex - Frauda (art.215 c.p./ licitaţiile pe eBay), Şantajul (art.197 c.p.), Falsul de monedă (art.282/284 c.p.).

INFRACŢIUNI PREVĂZUTE PRIN LEGEA COMERŢULUI ELECTRONIC (NO. 365/2002) REFERITOARE LA INSTRUMENTELE ELECTRONICE DE PLATĂ

- falsificarea cardurilor de credit

- utilizarea fără drept a unui card de credit sau a informaţiilor referitoare la un card de debit/ credit
- fabricarea ori deţinerea de echipamente, inclusiv hardware sau software, cu scopul de a servi la falsificarea instrumentelor de plată electronică etc. (art.24-28)

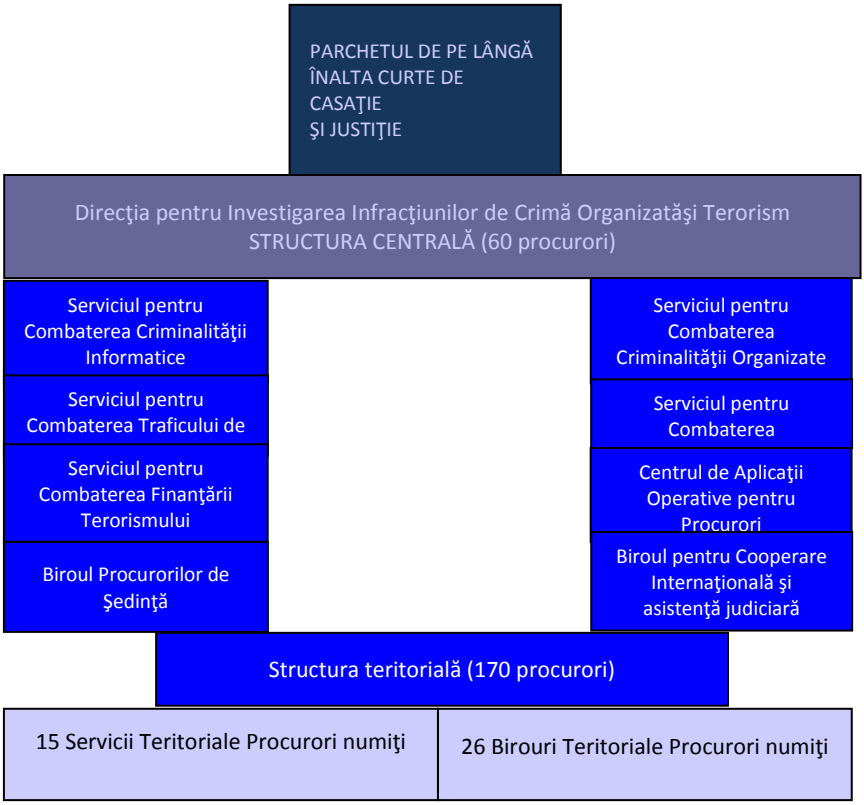
INFRACŢIUNI PREVĂZUTE PRIN LEGEA NR. 8/ 1996, actualizată

Ex. art.139/1 – reproducerea fără drept a unui program de calculator într-un sistem informatic prin intermediul oricărui tip de instalare sau executarea unei comenzi etc.

MIJLOACELE SPECIALE DE INVESTIGAŢIE prevăzute în CPPR şi legile speciale

- Lucrătorii sub acoperire/ colaboratorii/ informatorii
- Interceptările telefoanelor
- Interceptările traficului de internet/ comunicaţiilor sau păstrarea datelor
- Accesul într-un sistem informatic
- Percheziţia domiciliului
- Percheziţia informatică
- Supravegherea unui cont bancar/ a informaţiilor primite de la bănci
- Indisponibilizarea/ confiscarea bunurilor

STRUCTURA NAŢIONALĂ A PARCHETELOR SPECIALIZATE



PREROGATIVE ŞI COMPETENŢE
DIICOT îşi desfăşoară investigaţiile în dosare de infracţiuni grave, după cum sunt definite în Legea nr. 39/2003 privind combaterea criminalităţii organizate, precum şi la Articolul 12 al Legii nr. 508/2004:

- infracţiuni de crimă organizată;
- infracţiuni împotriva securităţii naţionale;
- infracţiunile de terorism şi de finanţare a terorismului;
- criminalitate informatică;

- infracţiuni în domeniul proprietăţii intelectuale şi industriale, dacă făptuitorii aparţin unor grupări de crimă organizată sau s-au asociat şi şi-au înfiinţat grupuri în vederea comiterii de infracţiuni;
- frauda cu carduri de credit şi infracţiuni conexe;
- traficul de droguri şi consumul de droguri ilegale;
- traficul de fiinţe umane; traficul de ţesuturi, celule şi organe umane;
- infracţiuni de contrabandă prevăzute în Codul Vamal al României;
- infracţiuni de spălare de bani, dacă banii, bunurile şi valorile reprezentând obiectul spălării de bani provin din producerea de infracţiuni aflate în competenţa DIICOT.

SERVICIUL PENTRU COMBATEREA CRIMINALITĂŢII INFORMATICE

(Unitatea de combatere a criminalităţii informatice)

- furnizează asistenţă specializată pentru celelalte autorităţi străine;
- dispune păstrarea de îndată a datelor informatice sau de trafic;
- execută sau facilitează executarea de comisii rogatorii sau a altor cereri de asistenţă judiciară reciprocă în dosare de criminalitate informatică prin care se solicită:
    - identificarea persoanelor
    - certificate de cazier judiciar
    - adrese sau furnizori de IP
    - percheziţii domiciliare sau informatice
    - interceptarea tuturor tipurilor de comunicaţii
    - indisponibilizarea sau blocarea activelor
- **investighează dosare complexe, tehnice de criminalitate informatică**

O structură similară a fost instituită în 2003 în cadrul Poliţiei Naţionale Române – Unitatea de Combatere a Criminalităţii Informatice în cadrul Direcţiei pentru Investigarea Infracţiunilor de Crimă Organizată/ Inspectoratul General al Poliţiei Române

FACTORI OBIECTIVI ŞI SUBIECTIVI CARE AU FAVORIZAT CRIMINALITATEA INFORMATICĂ ÎN ROMÂNIA

- accesul din ce în ce mai răspândit la echipamente şi conexiuni rapide şi moderne (în ultimii 2 ani);
- conexiunile anonime, dificultăţile de cooperare cu furnizorii de servicii, cafenelele internet, reţelele campus-urilor universitare sau reţele mici;
- relativa uşurinţă cu care se pot desfăşura anumite acte specifice criminalităţii informatice;
- reacţia întârziată cu privire la celelalte autorităţi naţionale sau internaţionale,
- lipsa previzibilităţii în ceea ce priveşte urmărirea penală şi, de asemenea, procedurile din instanţă

Anexa VII – Formular de solicitare a datelor de trafic

Formularul din paginile care urmează a fost elaborat în cursul proiectului pentru agenţiile autorizate să solicite date de la deţinătorii de date cu caracter personal.

SOLICITARE DE DATE DE TRAFIC

Prezentul formular trebuie completat pe hârtie cu antetul instituţiei dvs.

Organizaţia ţintă

Organizaţia ţintă	
Denumirea firmei (dacă se cunoaşte)	Click aici pentru a insera textul.
Denumirea juridică:	Click aici pentru a insera textul.
Persoană de contact	
Numele persoanei de contact:	Click aici pentru a insera textul.
Funcţia persoanei de contact:	Click aici pentru a insera textul.
Adresa persoanei de contact:	Click aici pentru a insera textul.
Ţara:	Se alege numele unei ţări.

Telefonul persoanei de contact:	Click aici pentru a insera textul.	Fax:	Click aici pentru a insera textul.
Adresa de e-mail de contact	Click aici pentru a insera textul.	Telefon mobil:	Click aici pentru a insera textul.

Instituţia Sursă

Instituţia solicitantă	
Denumirea de activitate a instituţiei	Click aici pentru a insera textul.
Denumirea juridică a instituţiei (dacă este diferită)	Click aici pentru a insera textul.
Denumirea unităţii instituţiei (dacă este diferită)	Click aici pentru a insera textul.
Codul de referinţă al instituţiei:	Click aici pentru a insera textul.
Categorie:	Parchet

Contactul instituţional principal		**Contactul instituţional secundar**	
Codul persoanei	Click aici pentru a insera textul.	Codul persoanei	Click aici pentru a insera textul.
Nume:	Click aici pentru a insera textul.	Nume:	Click aici pentru a insera textul.
Funcţie:	Click aici pentru a insera textul.	Funcţie:	Click aici pentru a insera textul.
Adresă	Click aici pentru a insera textul.	Adresă	Click aici pentru a insera textul.
	Click aici pentru a insera textul.		Click aici pentru a insera textul.

Ţara:	Se alege numele unei ţări.	Ţara	Se alege numele unei ţări.
Telefon:	Click aici pentru a insera textul.	Telefon	Click aici pentru a insera textul.
Fax:	Click aici pentru a insera textul.	Fax:	Click aici pentru a insera textul.
e-mail	Click aici pentru a insera textul.	e-mail:	Click aici pentru a insera textul.
Telefon mobil:	Click aici pentru a insera textul.	Telefon mobil:	Click aici pentru a insera textul.
Program de lucru:	Click aici pentru a insera textul.	Program de lucru:	Click aici pentru a insera textul.
Fus orar:	Click aici pentru a insera textul.	Fus orar:	Click aici pentru a insera textul.

Solicitare de date de identificare			
Data/ ora solicitării	Click aici pentru a alege o dată.	Ora:	Click aici pentru a insera textul.
Codul dosarului			
Numărul dosarului	Click aici pentru a insera textul.	Confidenţialitate & Clasificare	Se alege un articol.
Codul unic de referinţă (Instituţia solicitantă)	Click aici pentru a insera textul.	Codul unic de referinţă (Organizaţia ţintă)	Click aici pentru a insera textul.
ESTE URGENT?	☒	DATA SOLICITĂRII	12-Dec-11
Explicarea priorităţii	Minorul a dispărut după ce a participat la activitatea din camera de chat. Sunt necesare detalii.		

Verificare - Autoritate – Domeniu de cuprindere

Legislaţia aplicabilă		**Rolul solicitantului/ contact**	
Titlul din legislaţie	Click aici pentru a insera textul.	Activitatea instituţiei	Click aici pentru a insera textul.
Articole relevante	Click aici pentru a insera textul.	Funcţia juridică a agenţiei	Se alege un articol.
Dreptul de a solicita date	Click aici pentru a insera textul.	Ştampila oficială a organizaţiei	
Coduri de practici	Click aici pentru a insera textul.		
Hotărâri relevante ale instanţei	Click aici pentru a insera textul.	Data	Click aici pentru a alege o dată.
Autorizaţii verificate anterior		**Elemente specifice privind infracţiunea**	
Codul ofiţerului	Click aici pentru a insera textul.	Gravitatea infracţiunii investigate, pentru a permite comparaţia dintre diferitele legislaţii naţionale	
Codul SPOC	Click aici pentru a insera textul.		
Convine să nu publice informaţii confidenţiale de afaceri	Se alege un articol.	Click aici pentru a insera textul.	

Detaliile de verificare ale managerului		**LISTA DE CONTROL DE CĂTRE MANAGER**	
Nume:	Click aici pentru a insera textul.	Verificarea calităţii	Se alege un articol.
Titlul	Click aici pentru a insera textul.	Evaluarea impactului colateral	Se alege un articol.
Funcţia:	Click aici pentru a insera textul.	Evaluarea proporţionalităţii	Se alege un articol.
Semnătura:		Evaluarea consecinţelor asupra costurilor?	Se alege un articol.

Specificaţii disponibile privind datele (SE ADAUGĂ FOI SEPARATE PENTRU CONTURILE SUPLIMENTARE)

Vă rugăm să descrieţi pe scurt cazul				
Click aici pentru a insera textul.				
Adresa IPv4	1-255	1-255	1-255	1-255
	Click aici pentru a insera textul.	Click aici pentru a insera textul.	Click aici pentru a insera textul.	Click aici pentru a insera textul.
Data	Click aici pentru a alege o dată.		Ora	Click aici pentru a insera textul.
Fus orar	Click aici pentru a insera textul.			

Specificaţii privind adresa e-mail			
Adresa e-mail	Click aici pentru a insera textul.	@	Click aici pentru a insera textul.
Data	Click aici pentru a introduce data.	Ora	Click aici pentru a insera textul.
Fus orar	Click aici pentru a insera textul.		

Adresa IPv6	Subnet – 64bit	Host – 64bit	
	Click aici pentru a insera textul.	Click aici pentru a insera textul.	
Data	Click aici pentru a alege o dată.	Ora	Click aici pentru a insera textul.
Fus orar	Click aici pentru a insera textul.		

Reţele sociale & Servicii de comunicare online	
ID serviciului (Skype, Windows Live, Chat room, etc.)	Click aici pentru a insera textul.

ID serviciului de reţea socială (Bebo, Facebook, etc.)	Click aici pentru a insera textul.		
Persoana/ Organizaţia			
Numele companiei (dacă se cunoaşte)	Click aici pentru a insera textul.		
Denumirea juridică:	Click aici pentru a insera textul.		
Persoana de contact			
Numele persoanei de contact:	Click aici pentru a insera textul.	Numărul de cont:	Click aici pentru a insera textul.
Funcţia persoanei de contact:	Click aici pentru a insera textul.		
Adresa:	Click aici pentru a insera textul.		
Ţara:	Se alege numele unei ţări.		
Telefon:	Click aici pentru a insera textul.	Fax:	Click aici pentru a insera textul.
E-mail de contact	Click aici pentru a insera textul.	Telefon mobil:	Click aici pentru a insera textul.

Date solicitate FURNIZORUL DE SERVICII ELECTRONICE

Perioada de interes			
Data/ ora iniţiale	Click aici pentru a alege o dată.	Data/ ora finale	Click aici pentru a alege o dată.

Date privind abonatul					
Contactul principal	☐	Adresa de furnizare a serviciului	☐	Servicii acceptate	☐
Echipament instalat	☐	Software achiziţionat	☐	Servicii online furnizate	☐
SNS Prieteni	☐	SNS Interacţiuni publice	☐	Loguri SNS	☐

Date de trafic **Datele disponibile depind foarte mult de serviciu şi de ţară şi nu toate datele sunt disponibile**			
Şapouri e-mail	către/de la/dimensiune	trimise/primite - data/ ora/ fus orar	☐
Date trafic	Adresa IP, data/ ora/ fus orar		☐
Date trafic net	Pagini solicitate, cookies stocate şi valori, data/ ora/ fus orar		☐
Date apeluri	Date SMS, număr apelat, număr apelant, durată, statut, numere IMEI, coduri SIM, data/ ora/ fus orar, reţele de roaming, mesagerie vocală, blocarea apelurilor, redirecţionarea, mobile folosite, acoperirea semnalului		☐
Date FTP	Titlul fişierelor încărcate, descărcate, adresele IP, nume de utilizator/ parole		☐

Date de facturare	
Perioada de facturare	☐
Metoda de plată	☐
Adresa de facturare	☐
Istoricul plăţilor	☐

Date privind dispozitivul			
Date privind IMEI	☐	Adresa MAC	☐
Funcţii	☐	Producător	☐
Software	☐	Tip	☐
Model	☐		

Date privind contactul					
Data începerii	☐	Opţiuni de plată	☐	Servicii încetate	☐
Data finalizării	☐	Reguli privind respectarea dreptului la viaţă personală şi confidenţialitate	☐	Istoricul apelurilor de sprijin	☐
Echipament CPE	☐	Servicii acceptate	☐		☐

Date organizaţionale relevante					
Localizările punctelor de acces	☐	Arhitectura reţelei	☐	Contacte juridice	☐
Localizările celularului	☐	Echipament CPE	☐	Ghidul OAL	☐
Staţiile de antene GSM	☐	Locul unde sunt stocate datele relevante pentru caz	☐		

Alte informaţii specifice, rugăm fiţi concişi, clari, precişi şi la obiect
Click aici pentru a insera textul.

Date Solicitate FURNIZORUL DE TELECOMUNICAŢII

Perioada de interes			
Data/ ora iniţiale	Click aici pentru a alege o dată.	Data/ ora finale	Click aici pentru a alege o dată.

Date de abonat					
Contactul principal	☐	Adresa de furnizare a serviciului	☐	Servicii acceptate	☐
Echipament instalat	☐	Software achiziţionat	☐	Servicii online furnizate	☐
SNS Prieteni	☐	SNS Interacţiuni publice	☐	Loguri SNS	☐

Date de trafic Datele disponibile depind foarte mult de serviciu şi de ţară şi nu toate datele sunt disponibile			
Şapouri e-mail	către/de la/dimensiune	trimise/primite - data/ ora/ fus orar	☐
Date trafic	Adresa IP, data/ ora/ fus orar		☐
Date trafic net	Pagini solicitate, cookies stocate şi valori, data/ ora/ fus orar		☐
Date apeluri	Date SMS, număr apelat, număr apelant, durată, statut, numere IMEI, coduri SIM, data/ ora/ fus orar, reţele de roaming, mesagerie vocală, blocarea apelurilor, redirecţionarea, mobile folosite, acoperirea semnalului		☐
Date FTP	Titlul fişierelor încărcate, descărcate, adresele IP, nume de utilizator/ parole		☐

Date de facturare	
Perioada de facturare	☐
Metoda de plată	☐
Adresa de facturare	☐
Istoricul plăţilor	☐

Date privind dispozitivul			
Date privind IMEI	☐	Adresa MAC	☐
Funcţii	☐	Producător	☐
Software	☐	Tip	☐
Model	☐		

Date privind contractul					
Data începerii	☐	Opţiuni de plată	☐	Servicii încetate	☐
Data finalizării	☐	Reguli privind respectarea dreptului la viaţă personală şi confidenţialitate	☐	Istoricul apelurilor de sprijin	☐
Echipament CPE	☐	Servicii acceptate	☐		☐

Date organizaţionale relevante					
Localizările punctelor de acces	☐	Arhitectura reţelei	☐	Contacte juridice	☐
Localizările celularului	☐	Echipament CPE	☐	Ghidul OAL	☐
Staţii de antene GSM	☐	Locul unde sunt stocate datele relevante pentru caz	☐		

Alte informaţii specifice Vă rugăm să fiţi concis, clar, precis şi concentrat
Click aici pentru a insera textul.

Date Solicitate Instituţia financiară

Perioada de interes			
Data/ ora iniţiale	Click aici pentru a alege o dată.	Data/ ora finale	Click aici pentru a alege o dată.

Date privind abonatul					
Contactul principal	☐	Adresa de furnizare a serviciului	☐	Servicii acceptate	☐
Dispozitiv de logare/ echipament	☐	Software achiziţionat	☐	Servicii online furnizate	☐
Emiteri de carduri	☐	Numerele cardurilor	☐		

Date de trafic Datele disponibile depind foarte mult de serviciu şi de ţară şi nu toate datele sunt disponibile			
Şapouri e-mail	către/de la/dimensiune	trimise/primite - data/ ora/ fus orar	☐
Date trafic	Adresa IP, data/ ora/ fus orar		☐
Date trafic net	Pagini solicitate, cookies stocate şi valori, data/ ora/ fus orar		☐
Date apeluri	Date SMS, număr apelat, număr apelant, durată, statut, data/ ora/ fus orar		☐
Date FTP	Titlul fişierelor încărcate, descărcate, adresele IP, nume de utilizator/ parole		☐
Date CCTV	Data/ ora/ fus orar, imagini de la ATM etc.		☐
Date tranzacţii	Data/ ora/ fus orar, date tranzacţie, valoarea tranzacţiei, detaliile plătitorului, cont		☐

Date de facturare/ extras			**Date privind dispozitivul**			
Perioada de facturare	☐		Date privind IMEI	☐	Adresa MAC	☐
Metoda de plată	☐		Funcţii	☐	Producător	☐
Adresa de facturare	☐		Software	☐	Tip	☐
Istoricul plăţilor	☐		Model	☐		

Date privind contractul					
Data începutului	☐	Opţiuni de plată	☐	Servicii încetate	☐
Data finalizării	☐	Reguli privind respectarea dreptului la viaţă personală şi confidenţialitate	☐	Istoricul apelurilor de sprijin	☐
Echipament CPE	☐	Servicii acceptate	☐		☐

Date organizaţionale relevante					
ATM/Bancă localizări	☐	Arhitectura reţelei	☐	Contacte juridice	☐
Locul unde sunt stocate datele relevante pentru caz	☐	Echipament CPE	☐	Ghidul OAL	☐

Alte informaţii specifice Vă rugăm să fiţi concis, clar, precis şi concentrat
Click aici pentru a insera textul.